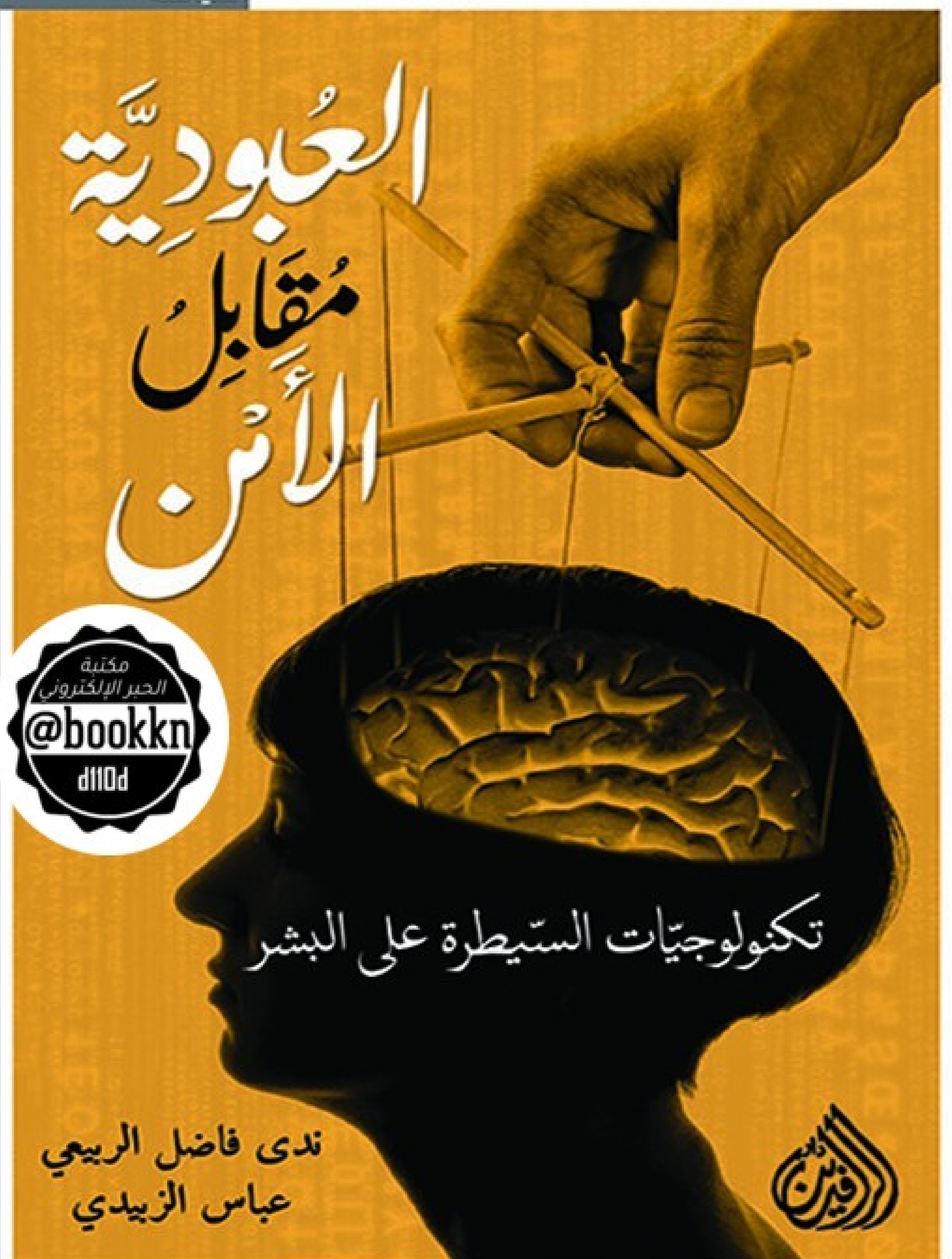
سياسة


العُبودِيَّة
مُقابِلَ
الأَمْن
تكنولوجيّات السّيطرة على البشر
ندى فاضل الربيعي
عباس الزبيدي
مكتبة
الحبر الإلكتروني
@bookkn

العبودية مقابل الأمن

تكنولوجيات السيطرة على البشر

العبودية مقابل الأمن
تكنولوجيات السيطرة على البشر

ندى فاضل الربيعي
عباس الزبيدي

*Zubaidi**By Nada Fadhil Al-rubaiee & Abbas Al-***

الطبعة الأولى: أكتوبر - تشرين الأول، 2020 (1000 نسخة)



لبنان ـ بيروت / الحمرا
تلفون: 345683 1 961+ / 541980 1 961+
بغداد ـ العراق / شارع المتنبي عمارة الكاهجي
تلفون: 9647714440520+ / 9647811005860+
info@daralrafidain.com
daralrafidain@yahoo.com
www.daralrafidain.com
dar alrafidain
Dar.alrafidain
دار الرافدين@daralrafidain

تنبيه: إن جميع الآراء الواردة في هذا الكتاب تعبّر عن رأي كاتبها، ولا تعبّر بالضرورة عن رأي الناشر.

ISBN: 978 - 9922 - 634 - 45 - 6

العبودية مقابل الأمن
تكنولوجيات السيطرة على البشر

ندى فاضل الربيعي
عباس الزبيدي

ندى فاضل الربيعي
عباس الزبيدي



www.daralrafidain.com

الفهرس

إهداء...

إلى من يهمه الأمر!

مقدمة تمهيدية

راودتني فكرة هذا الكتاب عام 2012 مع بداية احتكاكي الفعلي ببعض المواضيع التي تخص الصحة في بلد إقامتي - هولندا - كان ذلك قبل ثمانية أعوام من الآن حين كنت أعمل على تفعيل الملفات الإلكترونية للمرضى الذين يرتادون مراكزي الصحية الثلاثة في مدينة روتردام، والاحتكاك جاء مع بدء تطبيقنا نظامًا جديدًا لحفظ ملفات المرضى الصحية وجعلها متاحة لكافة الجهات المتخصصة وذلك بطلب من وزارة الصحة. أسئلة كثيرة لم تكن تفارقني أثناء عملي اليومي حول الهدف الحقيقي خلف فرض هذه المسألة على المواطنين المرضى؛ الأمر الذي دفعني إلى التعمق في تفاصيل التقنية الجديدة ومحاولة فهمها أولاً ومن ثم محاولة الكشف عن خباياها والبحث عمّا إذا كان للموضوع علاقة لما شهدَتْه الساحة الأوروبية والعالمية من تغييرات في العقد الأول من هذا القرن قبل بضعة سنوات توجّه النظام الصحي الهولندي في الصيدليات العامة والخاصة إلى توثيق كل ما يتعلق بالمريض من علاجات وأمراض، الأمر كان لا يقتصر على المرضى الذين يرتادون صيدلية الحي فقط بل يشمل كل رواد المراكز الصحية والعيادات والمستشفيات، حيث باشرت الحكومة الهولندية العمل بمشروع «الملف الصحي الإلكتروني» الشامل بموجب هذه التقنية يتم توثيق الملف الصحي للمريض وفتحه أمام كافة السلطات «الصحية»؛ ليتمكن في إطار هذا المشروع أي من العاملين في المجال الصحي في هولندا الاطلاع على الملف الصحي لأي مواطن.

تقوم الموظفة في الصيدلية بتقديم شرح مختصر للمريض حول أهمية الموافقة على تبادل المعلومات الصحية وحفظها في ملف إلكتروني؛ أثر هذا الشرح يدلي المريض بقبوله أو رفضه لإعطاء موافقة يُسمح بموجبها؛ لمن يشاء بالاطلاع على تفاصيل حياته الصحية، الأسباب التي تقدمها الموظفة هي الأسباب التي طلبت وزارة الصحة ذكرها، ومن أهمها أنّ الطبيب المعالج في حالات الإسعاف وزيارة المستشفى يستطيع الاطلاع على ملف المريض؛ لعلاجه كما يجب وذلك

بغض النظر عن مكان إقامة المريض أو المدينة التي يرتاد فيها المشفى، بعد مُضي أكثر من ثمانية أعوام تقريبا منذ أن بدأت بتطبيق هذا المشروع، أكثر ما أثار انتباهي ودهشتي هو أنّ الأغلبية الساحقة تعاملت مع الموضوع بسلاسةٍ شديدةٍ لافتةٍ للنظر ولم يواجهني بالرفض سوى عشرات المرضى من أصل أكثر من 30000 مريض، البعض كان يعاني من انفصام بالشخصية وكان يأتي صباحًا للصيدلية بالموافقة ومن ثَمّ يأتي لاحقًا مساءً يلغي الموافقة، وبعد امتعاضنا من هذه الحالة ثبت لدينا رفضه القاطع، آخرون ممن رفضوا إعطاء موافقة؛ لفتح ملفهم الصحي هم أشخاص لهم ماضٍ معين كما الحال مع إحدى النساء التي كان لها ماضٍ في الجنس المدفوع خشية من الكشف عن أي تفصيلة ترتبط بماضيها الشخصي قامت برفض التوقيع، آخرون ممن يعانون من حالة خوف مزمن ومستعصية رفضوا، الأمر حقًّا لافتٌ للنظر. هل غرّد هؤلاء المرضى الرافضون لهذه التقنية خارج السرب؛ لأنهم بحالة نفسية وعصبية لا تسمح بموقف مغاير؟أم الماضي هو الذي يدفع الشخص للحذر والخشية؟لكن ماذا عن الباقين؟هل ليس لديهم ماضٍ أو شيء يخافون عليه من أن ينفضح؟هل هم على حق؟وهل تعاني الأغلبية الساحقة من استسلامٍ وثقةٍ عمياء بمجريات الأمور؟

منذ الوهلة الأولى وهناك سؤال يؤرقني عن أهمية هذا المشروع وعن حاجتنا الحقيقة له إنْ وُجدت أصلًا، إنْ كنت أنا مريضة لا أرتاد سوى الصيدلية التي في الحي ولا أغادر مدينتي، لماذا يكون ملفي الصحي الإلكتروني مباحًا للاطلاع عليه من قبل «المختصين» في هولندا قاطبة؟، هل يوجد بالفعل حاجة لشيءٍ من هذا القبيل؟أليس بالإمكان أن يتم سؤال المريض في حال تواجده في مكان آخر ما إذا كان يسمح بطلب ملفه من الصيدلية «الأم»؟ولكن إن كان المشروع حقًّا فعالًا وفي صالح المريض ما هي مخاطر تسجيل كل شاردة وواردة عن حياة المواطنين الصحية؟، هل نحن بالفعل نحتاج لنظامٍ يتم من خلاله حفظ كل هذه التفاصيل وجعلها في الآن ذاته مفتوحة «للجميع»؟ أثر مشاهداتي اليومية نشأت لديّ الرغبة للتعمق في هذا الموضوع والبحث عمّا يحيط به من أسرار، في خضم بحثي وجدت نفسي فجأةً في بحيرة أسرار وفضائح «جوليان أسانج» كما وجدتُني أغوص في دوامة جوجل وإدوارد سنودن، وبدأت أسترجع بعض الإجراءات التي شهدتْها الساحة الهولندية والدولية فيما يخص الحريات العامة وبدأت الأسئلة تتكاثر، ووجدت نفسي أنتقل من مسألةٍ بدتْ شكليةً تخصّ الصحة العامة إلى مواضيع أكثر عمقًا وخطورة. أثناء بحثي ظهرت أمامي أمور كثيرة بعيدة في ظاهرها عن مجال الصحة ولكنها في الصميم في مجال حرية الأفراد، وغرقت في أسئلةٍ عن تحالف العيون الخمس، من هم؟ومن هم إدوارد سنودن وجوليان أسانج؟وما أهمية ما قام به؟

وكيف كانت بداية الشركات الأمنية؟وما هي حقيقة دورها المزعوم في حماية ما يسمى بالحريات الشخصية للأفراد؟ولماذا تغزو سماء الكوكب طائراتٌ من دون طيار؟وما هي البطاقات الجزيئية والممغنطة؟وما هو شكل المستقبل في ظل هذه التقنية؟، وأخيرًا، ما هو مفهوم الأمن العام؟وما معنى مفهوم حماية الفرد من الأخطار الخارجية في ظل مجتمع آمن؟أثناء بحثي الذي استمر لسنواتٍ تواصلتُ مع الدكتور العراقي عباس الزبيدي وهو مهندس طبي عراقي، عمل كمصمم لأنظمة التصوير الطبي لحساب وكالة الفضاء الكندية (CSA) وباحث في جامعة ساسكاتشوان الكندية واتفقنا على التعاون؛ لإكمال هذا البحث، الدكتور عباس أثرى البحث بمعرفته ومعلوماته القيمة عن الذكاء الاصطناعي، التعاون والبحث المتواصل استمر لأكثر من عام إلى أن وصلنا إلى الكتاب بصيغته الحالية.

ندى فاضل الربيعي - هولندا 2020

مدخل الكتاب

استمرت فكرة العقل البشري باعتباره المجال النهائي للحماية المطلقة من التسلل الخارجي لعدة قرون، لكن ما مدى صحة هذه الفكرة الآن؟ومن يضمن حمايتنا لعقولنا؟وهل لدينا القدرة على السيطرة على عقولنا؟وهل من إثباتات على خروقات أو سيطرة ما عليها؟في القرن الماضي وبالتحديد عام 1913، كتب المؤرخ جون بانفيل ما يلي: «لا يمكن أبدًا إعاقة أي رجل عن التفكير في أي شيء يختاره طالما يخفيه»! وفي فكرة موازية صوّر جون ميلتون عام 1634 في قصته القصيرة مشهدًا مذهلًا حيث تمّ تقييد امرأة شابة بكُرسي اعتراف للسحرة من قِبل رجل فاسق يُدعى: كوموس، في هذا المشهد الأسطوري تصرخ المرأة وتخاطب كوموس قائلة: «لا يمكنك أن تلمس حرية عقلي»! لقد كانت واثقةً تمامًا من قدرتها على حماية حريتها العقلية من أي تلاعب خارجي! ربما كان ما قاله بانفيل، أو ما تخيله ميلتون حقيقيًّا حينها، لكن ما هو الحال الآن وهل العقل بعيد عن سيطرة الآخرين؟وهل صاحبه قادرٌ على الحفاظ عليه؟

مع كل التطورات المتسارعة في التقنيات المعقدة، فإن هذا الافتراض باعتقادنا وكما سوف يوضح هذا الكتاب في طياته لم يعد قائمًا؛ إذْ تتيح الأجهزة العصبية المتطورة، مثل التصوير العصبي المتطور وواجهات الكمبيوتر الدماغية (BCI)، تسجيل الارتباطات العصبية للعمليات العقلية وفك تشفيرها وتعديلها والإضافة الشاملة أو الجزئية عليها، وتتسارع إشارات الأبحاث إلى أنّ الجمع بين تقنية التصوير العصبي والذكاء الاصطناعي يسمح لـ«قراءة» وربط الحالات الذهنية بما في ذلك النوايا الخفية والتجارب البصرية أو حتى الأحلام بدرجة متزايدة من الدقة، إضافة إلى تقنيات فك تشفير المعلومات العقلية عن طريق التصوير العصبي الوظيفي (fMRI) في استعراض الأدلة الجنائية لقضيةٍ ما أمام المحكمة والسلطات القضائية أو التحقيقية الأخرى، فعلى سبيل المثال، في عام 2008، أُدينت امرأة هنديّة بالقتل وحُكم عليها بالسجن مدى الحياة على أساس فحص

مسبري للدماغ (Brain scan)، وفقًا للقاضي، فإنّ صور التصوير المقطعي من دماغ المرأة المشتبه بها كان يحتوي بوضوح «المعرفة التجريبية» حول تلك الجريمة، وفي ذات السياق أثارت إمكانات التكنولوجيا العصبية كأداة في الطب الشرعي اهتمامًا خاصًا فيما يتعلق بالكشف عن الكذب والنيات الشخصية الجرمية؛ لأغراض الاستجواب، على الرغم من شكوك الخبراء، فإن الشركات التجارية مثل «FMRI - Lie - No وGouvernement Works Inc تقوم بتسويق استخدام تقنية تستند إلى fMRI وEEG للتأكد من الحقيقة والباطل عبر تسجيلات الدماغ، في موازاة ذلك، تختبر القوات المسلحة الأمريكية تقنيات المراقبة العصبية لاكتشاف أوجه القصور الوظيفي أو التشريحي في نشاط الدماغ لدى المقاتل واستخدام تحفيز المخ؛ لزيادة تنبيههم واهتمامهم.

على الرغم من أن هذه التطورات تنطوي على إمكانات كبيرة في مجالات البحوث العلمية والطبية، فإنها تشكل تحديًّا أخلاقيًّا وقانونيًّا واجتماعيًّا، أو تحت أي ظروف، الوصول إلى النشاط العصبي لشخص آخر أو التدخل فيه وسبر أسراره، وهنا يكون التساؤل حول معنى الخصوصية والحرية جوهريًّا جدًّا. في عام 2015، أصدرت مجلة Science الأمريكية عددًا خاصًّا بعنوانٍ ملتهبٍ أثار موجة لا تنتهي من الجدل «نهاية الخصوصية» سلّط المقال الضوء على كيفية طرح الاتجاهات التكنولوجية الجديدة من البيانات الكبيرة (Big data) إلى اتصالات الإنترنت في كل مكان، بحيث يصبح الجزء أو الفرد منضمًّا للكل عنوةً، ففي هذا العالم الرقمي الجديد يجب على الجميع قبول الاستنتاج التالي: أنّ كل اتجاه تكنولوجي - رقمي يتم إنتاجه؛ يؤدي حتمًا إلى تآكل خصوصيتنا الضئيلة أصلًا في العالم الرقمي، حيث باتت المفاهيم التقليدية للخصوصية باليةً ولا مكان لها في هذا العالم الرقمي، وهناك القليل من الجهد الذي يمكننا القيام به حيال ذلك، نحن نعلم أننا - وربما جميعا - لسنا على استعدادٍ بَعد لقبول هذا الاستنتاج؛ قد يتطلب هذا التحدي الأخلاقي إعادة تعريف حقوق الإنسان الحالية وحتى إنشاء حقوق إنسان جديدة خاصة بالوعي العقلي وخصوصية الأفكار الداخلية للإنسان، فالحق في الحرية المعرفيّة، والتي نُوقشت على نطاقٍ واسعٍ ومفصّلٍ بين مُحبِّي علوم الأعصاب والدراسات النفسية، من شأنه أن يمنح الأفراد اتخاذ قراراتٍ حرة ومختصة فيما يتعلق باستخدامهم للتقنية العصبية المتقدمة بما يرونه مناسبًا لحياتهم ومجتمعهم، من شأن تحديد وتعريف الحقّ في الخصوصية العقلية أن يحمي الأفراد من الاقتحام غير المرخص به من قِبل أطراف ثالثة لبيانات عقولهم وكذلك ضد المجموعة التي تنوي استخدام غير مصرح به لتلك البيانات، ولعل انتهاكات الخصوصية على المستوى العصبي - العقلاني تعد أكثر خطورة من

تلك التقنيات التقليدية؛ لأنها تتجاوز مستوى التفكير المنطقي، تاركةً الأفراد دون حماية من قراءة عقولهم بشكل لا إرادي من قبل الآخرين.

لا ينطبق هذا الخطر فقط على المشاركين في دراسات التسويق العصبي المفترسة والاستخدامات غير المتناسبة للتقنية العصبية في المحاكم، ولكن على الأفراد عمومًا أيضًا مع التوافر المتزايد لواجهات الدماغ والحاسوب المتصلة بالإنترنت، أصبح المزيد من الأفراد مستخدمين لأجهزة واجهات الكمبيوتر الدماغية، فعلى سبيل المثال لا الحصر، كشفت Facebook عن خطة لإنشاء واجهة تحويل الكلام إلى نصٍ في الدماغ؛ لترجمة الأفكار مباشرة من إشارات الدماغ إلى شاشة الكمبيوتر، متجاوزة الكلام والأطراف العليا المسؤولة عن تنفيذ واجبات الكتابة، هذا، وهناك محاولات مماثلة من قِبل كبار مزودي خدمات الاتصالات المتنقلة، وخاصة Samsung لتطوير هذه التقنية لتصل باعتقادنا إلى أن يحل التحكم في الدماغ محل لوحة المفاتيح والتعرّف على الكلام كوسيلة أساسية للتفاعل مع أجهزة الكمبيوتر. أخيرًا، قد يحفظ الحقّ في الاستمرارية النفسية للهوية الشخصية واستمرار حياتهم العقلية من دون تغيير خارجي غير معلن من قبل أطراف ثالثة، تلك الخصوصية الفردانية والاستمرارية النفسية هي قضية مهمة في سياق الأمن القومي لكل البلدان، حيث يمكن تبرير التدخلات الإلزامية لتغيير الشخصية في ضوء أهداف استراتيجية أكبر وحماية كبرى للأفراد والشخصيات المهمة من الاختراقات الخارجية، بالتعديلات أو التدخلات الدماغية التي تقلل من الحاجة إلى النوم مثلًا هي قيد الاستخدام في الجيش والقوات المسلحة الأخرى، ومن السهل تخيّل التدخلات التي تجعل أولئك الجنود أكثر عدوانية أو بلا خوف!

إن التقنيات الثورية التي ملأت حياتنا بمختلف تطبيقاتها منعتنا من رؤية الثغرات الصغيرة التي استغلتها الشركات وأسست لها حيث تمكنت هذه الشركات من صناعة تكنولوجيا خطيرة أدت إلى تغيير دراماتيكي في أنماط اتصالاتنا وحياتنا مع بعضنا البعض وحولتنا إلى مجرد حالات رقمية (Digital status) يتمُّ التحكم بها عن بُعد بل يتم التغرير بها في بعض الأحيان، إذْ باتت هذه الأجهزة كالفيروس الذي يخترق الأنسجة الحية فيفعل فعله المخرب فيها.

في العقود القليلة الماضية لم يكن من الممكن للغرباء أن يشاهدوا صورنا الشخصية ولا الاطلاع على المعلومات الخاصة بنا إلا من خلال ما نسمح به نحن فقط، ولكن غيّر الوصول التلقائي للإنترنت وشبكات التواصل الاجتماعي بشكل جذري طريقة حياتنا وحتى إدراكنا

للخصوصية الشخصية بفلسفتها ومداركها، وهذا بالضبط ما أراد القائمون على صناعة التقنيات الرقمية الوصول إليه، ففي الوقت الذي يوحى إلينا بأن تلك التقنيات تمنحنا الحرية وتحافظ على خصوصية الفرد والمنظمات، يتم الاختراق المنظم لخصوصية الهلامية. أين نحن من كل تلك الجرائم الرقمية أو السيبرانية والتي تُرتكب بحقنا على مسمعٍ ومرأى منا من دون أدنى رادع أو حاجز؟!

تلك القصص والسيناريوهات التي ملأت صفحات الجرائد والمجلات والمواقع الرقمية المتعددة حول خداع بعض شركات السمسرة لتجارة البيانات الشخصية التي كان لها الدور الفاعل في كسر أسوار خصوصية المجتمع والأفراد بشكل منظم على الرغم مِن أنّ هناك مَن يقول إنّ تلك الشركات أصلًا هي صنيعة الحكومات والأحلاف الجيوستراتيجية التي تكونت بعد الحرب العالمية الثانية وما يطلق عليه تحالف العيون الخمس، إضافة إلى مؤسسات التجسس الرسمية في روسيا، والصين والاتحاد الأوروبي، وتلك الدول غير المنضوية في تحالفات أمنية واستخباراتية عبر المحيطات. لقد تمّ خلق نظام شامل فيه نقاط مراقبة دائمة لمراقبة كل أنواع الاتصالات والمراسلات والبيانات وتحركات الأفراد والمجموعات وتسجيلها وتحليلها بشكل مستمر؛ لغرض رصد أي نشاط مشبوه يهدد الأمن القومي لتلك الدول والتحالفات أو يعمل على زعزعة الاستقرار الأمني والاقتصادي والاجتماعي والسياسي لها. إنه عصرٌ جديدٌ من المراقبة (Surveillance) لا بل عصر فكّ الشفرات (Decryption) للوعي البشري وتحليل أحجية وقدراته وتدعيمها بل واختراقها أيضًا، ربما يتم الآن تسجيل ومتابعة كل بياناتك التي تُدْلي بها بل ما لم تُدلِ به (بمعنى حتى المعلومات الصوتية المحيطة بك أيضًا)، ربما يستغرب البعض من ذلك ولكن هذه هي الحقيقة، إذ لم تعد المعلومات العقلية معزولة بل هي تحت المراقبة، وفكرة الذاتية في عقل شخص ما بدلًا من العالم الخارجي يصبح فارغًا، ويترتب على هذا كله تحديات اجتماعية جوهرية وخطيرة، فمن يحدد الحقوق التي يحقّ للأفراد ممارستها فيما يتعلق بالبُعد العقلي؟إلى أي مدى يحقّ للفرد أن يفكر، وما هو المسموح به للتفكير؟

سوف نحاول في هذه الدراسة الإجابة عن الكثير من الأسئلة رغم علمنا المسبق أنّ خيالنا لن يضاهي غرابة الواقع وغموض المستقبل؛ لذا سنتركم بين طيّات صفحات هذا الكتاب والذي نتمنى أن نكون قد غطينا فيه الكثير من المواضيع ذات الصلة بحرب الخصوصية والبيانات والأسلحة السيبرانية والخطر الداهم من انتهاك تلك الخصوصية المميزة لنا كجنسٍ بشري منتخب على كوكب

صغير، ونحاول في طيّات هذا الكتاب دمج المعلومة مع بعض الظواهر التي شهدها العالم بداية القرن الواحد والعشرين وذلك لقناعتنا بأن هذه الظواهر باتت ترسم ملامح العقد القادم بل وتؤسس لنظام اجتماعي جديد تنتفي فيه الحرية الشخصية أمام ما يسمى بالمصلحة العامة وتقوم الشركات الأمنية بالنيابة عن الدول بتسجيل وإحصاء تحركات الأفراد تحت ذريعة الحماية وتوفير الأمن العام للمجتمع والأفراد، ويتم تحت ذرائع مختلفة كالصحة العامة مثلا، إحصاء أنفاسنا وحساب تحركاتنا.

الكاتبان يعتبران هذا الكتاب صرخة ونداء للوعي من القادم، يأملان أن يصل صداها إلى من يهمه الأمر.

الفصل الأول

أسرار وتحالفات

1.1 من باحة الملهى إلى غرفة الاستخبارات

«هناك ثلاث مراحل في عملية إعادة تكاملك

هناك التعلّم والاستيعاب والتقبّل.

وقد حان الوقت؛ لأنْ نبدأ المرحلة الثانية»

جورج أورويل - رواية 1984

في نهاية القرن الماضي كتب الكثير عن رغبة الحكومة الأمريكية بتطبيق تقنيات جديدة أكثر دقة باتجاه جنود الولايات المتحدة الأمريكية لتعقب المتعطلين عن الخدمة مثلاً، أو لمتابعة المشرّدين داخل الولايات المتحدة الذين يعتمدون بشكل أو بآخر على مؤسسات الدولة أو المجتمع من أجل عيشهم، تمّ طرح فكرة المتابعة لهؤلاء الجنود الفارين والمواطنين المشرّدين من خلال استخدام تكنولوجيا حديثة مثل البطاقات الإلكترونية أو ما شابه، التي تُحقن أو تزرع في جسد هؤلاء بغية التتبع، لكنّ الأمر لم تتناوله وسائل الإعلام بتفاصيل كثيرة، وبدا لاحقًا وكأنما رغبة الولايات المتحدة لم تخرج إلى حيز التطبيق واقتصرت على أفلام هوليود، هل هذا صحيح؟هل تراجعت الولايات المتحدة عن استخدام هذه التقنيات لتعقب الأفراد؟أم أنها راحت تجرب أفكارها الجهنمية في أماكن أخرى؟إليكم هذه المفاجأة:

في مكانٍ بعيدٍ جغرافيًّا عن الولايات المتحدة وفي وقتٍ مبكرٍ من عام 2004 جاءت المفاجأة الأولى من قِبل أحد أشهر الملاهي الهولندية في مدينة روتردام، حيث قام صاحب الشركة باستخدام

تطبيقات إلكترونية لا بغرض معلن وهو «التتبع» بل لأسباب عملية أخرى كما ادّعى المسؤولون القائمون على هذا البرنامج، الغاية المعلنة من تطبيق التقنية في الملهى لم تُقنع الكثيرين ممّن تابعوا هذا الموضوع، من وجهة نظرنا فإنّ هذه التطبيقات تشكل بدايةً مرحلةٍ جديدةٍ هامةٍ سيتم الاستعانة بها في كافة المرافق في المستقبل. لكن ما هي هذه التطبيقات؟وهل يكون رواد الملهى حقل تجارب لأولئك الهاربين والمشرّدين؟وماذا عن العابثين والخارجين عن القانون؟

اقترح صاحب الملهى الهولندي فكرة الدفع في الملاهي عبر بطاقة إلكترونية تزرع تحت الجلد؛ الذريعة كانت السرقات التي يتعرض لها رواد الملاهي والمراقص ليلا، عرض صاحب الملهى على الحضور أن يتم زرع بطاقة إلكترونية بحجم حبة الأرز تحت جلدهم، ما يسمّى ب- RFID وهو اختصار باللغة الإنجليزية لمصطلح الرقاقات الراديو اللاسلكية Radio Frequency card - identi وهي عبارة عن شريحة صغيرة جدًّا مصنوعة من السليكون وهوائي؛ لكي يستطيع استقبال وإرسال البيانات والاستعلامات من خلال موجات الراديو، الفوائد التي ذكرها صاحب الملهى حول هذه التقنية هي كالآتي: «لم يعد من الضروري أن تحمل هوية التعريف بنفسك، بإمكانك الدخول للملهى وأن تمر جانب جهاز لاقط وسيتعرف الجهاز مباشرة إلى مَن تكون؟وكم من المال لديك كرصيد على البطاقة؟ستحظى لذلك بمعاملة خاصة وتدخل إلى أماكن لا يدخلها سوى الأشخاص المهمّين، بإمكانك أن تدفع الحساب مباشرة حيث يقرأ اللاقط كم الحساب ويتم سحب المبلغ من حسابك - بطاقتك -، عرضُ صاحبِ الملهى كان مغريًا، لقد عرض على الزبائن شحن البطاقة مجانًا بمبلغ من المال قدره «ألفان يورو»؛ ليتم إنفاقه في الملهى وسيكون لحامل الشريحة معاملة خاصة ومتميزة عن بقية الرواد، وبالفعل سرعان ما وافق في اليوم الأول - حسب الصحافة الهولندية - سبعون زائرًا دائمًا لهذا الملهى بحقن الشريحة من قِبل أحد الأطباء، سمحت لهم هذه البطاقة بدخول الملهى والحصول على معاملة خاصة بالأشخاص المهمين VIP. لقد عرضت المسألة على اعتبارها موضوعًا يجاري أحدث صراعات العصر والموضة ويؤمّن الحماية المادية للزبون، لقد تم تبسيط المسألة كذلك وعرضها على أنها تقدّم حلولًا لقضايا حياتية بسيطة، في استجواب قدّمه السيد مالينير عن الحزب اليميني في مدينة روتردام (لييف بار روتردام) Leefbaar Rotterdam ووجهه للبرلمان الهولندي في تاريخ 5 - 10 - 2004 حول استخدام تقنية الـ RFID في الملهى الهولندي في روتردام؛ وجّه السيد مالينير من خلال هذا الاستجواب سؤالين مفادهما الوصول إلى إجابة من الدولة حول المسألة: ما هي سياسة الدولة حيال هذه التقنية

في مجالات الصحة، والخصوصية والأخلاقية؟هل من مخطط الدولة لإصدار قوانين تنظم استخدام هذه التقنية؟جاءت أجوبة البرلمان ركيكة وغير حاسمة بشأن تعرض هذه التقنية لخصوصية الفرد أو تأثيرها على صحته. جاء في نص الإجابة: «إن اختيار الشخص لاستخدام هذه التقنية لا يختلف عن وضعه للوشم أو وضع الحُلي الحديدية في الجسد، وبما أن الموضوع يتم من خلال تغطية الفرد لنفقات هذه التقنية ويتم بشكل طوْعِي فلا يوجد هناك أي ضرورة تعديل القوانين وإصدار قوانين جديدة».

تجربة الملهى الهولندي هذه مثيرة للدهشة؛ لأنها تعرض في أساس الأمر حلولًا لمشكلات غير موجودة أصلًا أو مشكلات عارضة يكمُن حلها بعيدًا عن رواد الملهى، فبدلا من تأمين وتحصين رواد الملهى ضد السرقة يريد صاحبه برُوّاده أن يُحقنوا بتلك الشريحة؛ ليحموا أنفسهم من السرقة المادية! المثير في الموضوع كذلك أن الأمر وكما تبين لاحقًا لم يقتصر على المدينة الهولندية بل امتد إلى فرع الملهى في برشلونة المعروف بأنه من أكثر الملاهي شهرةً وازدحامًا، هناك في برشلونة تم الترويج للموضوع على شاشات التلفزة الإسبانية من قبل بعض المشاهير الذين سمحوا بحقنهم ببطاقة إلكترونية في أذرعهم وكما هو الحال مع كافة المواضيع المثيرة للجدل فلا يوجد حتى الآن أرقامٌ دقيقة حول عدد الأشخاص الذين تم حقنهم بتلك البطاقة، العدد الذي ذكرته الصحافة مشكوك به؛ خاصة وأن الرقم يخص فقط من تم حقنهم في ليلة الافتتاح ولم يشمل ما تلاها، أعتقد أن السنوات القادمة سوف تكشف عن وجود أرقام مذهلة.

حسنًا، لنفترض أن العشرات فقط من تم حقنهم، أين هؤلاء؟! هل من جهة تتابعهم أو تقوم بتحديث بياناتهم؟ومن يعرف أين تم تخزين تلك البيانات؟اللافت للنظر أن هذه التجربة لم يتم دراستها من قبل أية جهة رسمية أو أكاديمية. من خلال بحثنا الطويل عثرنا على دراسة وحيدة قامت بها جامعة وولونج الأمريكية بعنوان «استخدام شرائحالـ RFID كوسيلة للدخول إلى المباني والدفوعات: دراسة عن (بايا بيتش كلب) في برشلونة». أكد الباحثان ك وم ميشيل من خلال هذه الدراسة عدم وجود دراسات أخرى أو مراجع معتمدة تخص هذا التطبيق، من خلال بحثهم وتقصيهم اكتشف الباحثان أن الملهى له ثلاثة فروع منهما اثنان في أوروبا (روتردام وبرشلونة) والمركز الرئيسي في أمريكا، اللافت للنظر أن التقنية اقتصر تطبيقها على الدولتين الأوربيتين ولم يتم تجربتها في الولايات المتحدة! أجرى الباحثان لقاء مع مدير الملهى في برشلونة عام 2010 سألوه فيها عن فكرة التطبيق وأهدافه. شرح المدير فكرته حول هذا التطبيق

وأكد جازمًا أنه لا اختراق لحرية الأفراد وأنه لا يوجد أي مخاطر على صحتهم. بعد بضعة أشهر فقط من تجربة الملهى، يعلن مدير الفرعين الهولندي والإسباني عن إفلاسه وإغلاق أبواب الملهيين أمام الرواد، وأمام المحقونين بالشريحة؛ لنتساءل مرة أخرى عن هؤلاء. ما هو مصيرهم ومصير حبة الأرز تلك التي تحت جلودهم؟في العام الذي تلا أحداث الملهى تم تسجيل براءة اختراع مخترع سعودي لم ينشر اسمه، وتقوم براءة الاختراع هذه على الفكرة البسيطة والمذهلة التالية: المخترع تمكن من إجراء تعديل على شرائح الـ RFID بإضافة جرعة من السيانيد داخل البطاقة قبل الحقن، يتم حقن الأشخاص بهذه البطاقة الإلكترونية المزودة بالسيانيد، في حال خرج حاملها عن القانون تتمكن الجهات المعنية مِن التخلص منه بكبسة زر واحدة وعن بُعد! بحيث يخرج السيانيد ويتغلغل في جسد الشخص ويتم بالتالي القضاء عليه دون أن تسقط قطرة دم واحدة! اختراع جهنمي حقًّا! يبدو السؤال حول مَن سيستخدم هذا الاختراع غير ذي معنى فالكل سيكونون مهتمين به: السلطات وأجهزة الأمن والدول الكبرى والصغرى وحتى المجرمون الصغار والمافيات. قناة فوكس نيوز الأمريكية عرضت الاختراع بوصفه اختراعا يؤمّن إمكانية ملاحقة الإرهابيين والخارجين عن القانون والتخلص منهم. «إن لم تطع الأوامر أو إن خرجت عن قانوننا سنتخلص منك عن بُعد» هكذا نختصر هذه التقنية. بعيدا عن الملهى وروداه، في مكان آخر في القارة الأوروبية وبالتحديد في السويد أعلنت وكالة الأنباء المحلية APF عام 2018 أنّ آلافًا من الأشخاص حقنوا أنفسهم بشريحة إلكترونية؛ لاستخدامها في المواصلات والتعرّف على هويتهم كان هذا بالتعاون مع مركز Epicenter المعروف بتطبيقه لكل صراعات التكنولوجيا في السويد. لاحقا توالت الأنباء عن استخدام هذه الشرائح في بلدان عديدة من أمريكا اللاتينية إلى أمريكا وإفريقيا، الأسباب تعددت والنتيجة واحدة.

سوف نرى في ثنايا الكتاب تدريجيا علاقة هذه التقنية بما سوف يأتي من تقنيات أخرى. لقد كان جورج أورويل على حق، لقد حان الوقت الآن بالفعل لنبدأ مرحلة الاستيعاب، ما نمرُّ به اليوم يفوق مخيلة الجماهير، لقد تعلمنا الآن أهمية هذه البطاقات التي تزرع تحت الجلد لكن يجب الآن أن نستوعب ومن ثَمّ نتقبل فكرة حقنها تحت جلدنا!

1.2 صندوق سنودن والعيون الخمس

«لا أريد أن أعيش في عالمٍ يتمّ فيه مراقبة وتسجيل كل ما أقول، كل ما أفعل ومع مَن أتحدث، وكل ما أُعبّر عنه من مشاعر حبٍ أو إبداع»

- إدوارد جوزيف سنودن Edward Joseph Snowden 3
- 6 - 2013، في أول لقاء سِري مع الصحافة

تقوم أسطورة صندوق باندورا العجيب على أساس ارتكاب حماقة تتلخص بفتح صندوق العجائب هذا من قِبل مالكة الصندوق الذي كان يتوجب عليها عدم فتحه، لكنّ ظروفًا ما دفعت بطلة الأسطورة لفتحه فإذا بشرور الكون تنطلق من بين جوانب الصندوق وحواشيه، تقول الأسطورة: إنّ «زيوس تزوج من باندورا التي كانت تمتلك صندوقًا كان يجب عليها ألا تفتحه مطلقًا، غير أن باندورا فتحته فخرجت كل شرور البشر منه، أسرعت باندورا لإغلاق الصندوق، ولم يبقَ فيه إلا قيمة واحدة لم تخرج منه.... هي الأمل». تبادل سنودن وباندورا الأدوار في زواج جمعه مع الاستخبارات الأمريكية، كان من المفترض من سنودن أن يُبقي الصندوق مغلقًا لكنّ شيئًا ما دفع البطل هذه المرة أيضًا إلى كسر أغلال الصندوق والبوح بما في داخله، لم يدرك زيوس كما لم يدرك سنودن حجم الكارثة والهلاك القادمين مع هذه المغامرة العبثية، أو بالأحرى لم يستطع سنودن بعد أن فتح الصندوق سوى أن يقف؛ ليشهد هول ما يحدث إذْ بات منذ ذلك الحين هو كذلك عرضة لشظايا هذه الشرو. لن تكُفّ الأشرار بعد هذه اللحظة عن الخروج من هذا الصندوق العجيب! لقد خرجت الأمور عن سيطرة سنودن فلم يعُد يقوى على إغلاق الصندوق وإبعاد الشرور، أما الأمل الذي تبقى فهو أن يجد له مأوى آمنًا بعد أن ارتكب تلك الحماقة وتحطم عقد الزواج مع الاستخبارات الأمريكية.

ظهر سنودن إلى العلن عام 2013 مخلفًا زلزالًا استخباراتيًّا؛ حيث قام هذا الشاب الذي لم يبلغ عقده الثالث بتفجير قنبلة استخباراتية حين سرّب معلوماتٍ تتعلق بجمع وكالة الأمن القومي سجلات الهواتف الأمريكية ومراقبة اتصالات الإنترنت؛ اضطرت إثر هذا الحدث الولايات المتحدة الأمريكية للكشف عن بعض أخطر أوراقها وأشدها حساسية؛ مما دفع صحيفة وول ستريت جورنال الأمريكية يوم 28 أكتوبر بنشر خبرٍ مفادُه أنّ وكالة الأمن القومي الأمريكية اعترفت للمرة الأولى بالتجسس على 35 زعيمًا من زعماء العالم بما في ذلك التجسس على هواتفهم. وبدأت منذ تلك اللحظة الأحداث والأخبار تتوالى، الولايات المتحدة حاولت عبثًا تحجيم الشرور المنبعثة من فم سنودن.

كان هذا الشاب موظفًا في وكالة الاستخبارات المركزية الأمريكية ومتعاقدًا مع وكالة الأمن القومي. إدوارد سنودن من مواليد 21 - 6 - 1983 سرّب حسب الـ واشنطن بوست في تاريخ 9 - 6 - 2013 معلومات سرية للغاية من وكالة الأمن القومي وواجه إثر هذه الحادثة تُهمة وُجِهت إليه من قِبل القضاء الأمريكي رسميًّا في 21 يونيو 2013 بالتجسس وسرقة ممتلكات حكومية ونقل معلومات تتعلق بالدفاع الوطني دون إذن والنقل المتعمّد لمعلومات مخابرات سرية لشخصٍ غير مسموح له الاطلاع عليها، لم يكتفِ سنودن بالكشف عن عمليات تجسس منهجية طالت ملايين اتصالات الأوروبيين بل استمر بإطلاق المزيد من الأخبار الدّسمة؛ حيث أكد أن عمليات التجسس طالت حتى الهاتف المحمول للمستشارة الألمانية أنجيلا ميركل نفسها. سنودن الذي عمد على تسريب أكبر مشروع تجسس أمريكي في الإنترنت استطاع الهرب إلى روسيا وبدأ بعدها رحلة لم تخلُ من المصاعب للحصول على لجوءٍ سياسيٍّ؛ لكن لماذا؟ما قام به سنودن يضعنا اليوم أمام أسئلة جوهرية بالفعل: ما الذي دفع هذا الشاب ليفعل فعلته؟، ما الذي رآه؟، ما الذي دفع به لأخذ إجازة مرضية ومن ثمّ الهروب إلى المجهول؟كيف يندفع شاب في مقتبل العمر يعمل في الجهاز الاستخباراتي في الأمن القومي الأمريكي ويتقاضى راتبًا جيّدًا أن يرفض - لا - فكرة التجسس وحسب، بل وحتى فكرة السكوت على ما يراه؟ما الذي حدَا به لتحطيم عقد الزواج هذا؟ليبدأ فجأة رحلة يصارع فيها التجسس والمتجسسين ويقاتل؛ لإفشاء الحقائق! ما الذي دفع سنودن للمغامرة بحياته وترك حياة الرفاهية والاستقرار؟ليس السؤال المُلح، من أجل ماذا كان ما فعل؛ أعتقد أن السؤال الأكثر إلحاحاً هو ما الذي وقعت عليه عيناه وما الذي سمعه؟ما الذي أذهل هذا الشاب

وأخرجه عن صمته الاستخباراتي الذي طالما اعتمده كأساس في حياته وعمله كعميل ومتعاقد استخباراتي؟

لوك هاردنج صحفي وكاتب ومراسل جريدة الجارديان في الخارج عمل عدة تقارير عن الهند، روسيا، وألمانيا، كما أنه قام بتقديم عدة تقارير عن الحرب في أفغانستان، قدّم لوك كتابا ثريًّا بالمعلومات حول رحلة سنودن فسطّر في كتابه التواصل الأول بين سنودن والصحفي الأمريكي في صحيفة الجارديان جلين جرين، وتابع خطاه المتوالية منذ الْبوح بالسرّ إلى لحظات الهروب واللجوء. كان الصحفي جلين في البرازيل حين تلقى رسالة من جملة واحدة مفادها: «لدي وظيفة مرموقة في جهاز المخابرات» وذلك دون ذكر الاسم أو الوظيفة أو أية تفصيلة أخرى، توالت الرسائل بين الصحفي وسنودن، لكن الكثير من الشكوك راودت الصحفي حول هذه الشخصية الإلكترونية ولكنها سرعان ما وضحت الصورة وبدت شخصية وكأنها تملك الكثير من الوثائق والمعلومات، حسب الصحفي فإنّ سنودن بدَا عليه الهدوء والاستقرار الذهني والنفسي والعاطفي، «كان سنودن يعلم أن ما يكشفه من حقائق سوف يؤدي به إلى الاعتقال والمحاسبة لكن وجهه كان ينبض بالثقة والراحة، ما من شيء كان سيوقفه عن البوح بما يعرِف» قال سنودن للصحفي» لا أريد العيش في عالم يسجل فيه كل ما أفعل وما أفكر به ومع من أتحدث، مشاعري وإبداعاتي وحبِّي» وأضاف «هم كانوا مشغولين بحفظ كافة المعلومات التي تخص ملايين الأمريكيين دون الإعلان أو الاستئذان: مكالماتهم الهاتفية، بريدهم الإلكتروني وكل ما يبحثون عنه في شبكة المعلومات. من خلال هذا كله كان بإمكانهم تحديد صورة إلكترونية متكاملة عن هؤلاء المواطنين، من هم؟ومن أصدقاؤهم وشركاؤهم؟وماذا يفضلون؟وماهي مشاكلهم؟. عاش سنودن سنوات طفولته الأولى في ولاية شمال كارولينا حيث القاعدة البحرية، تربّى على أفكار قومية وليبرالية متحفظة، كان والد سنودن يعمل في حماية السواحل في كارولينا حيث أدّى القسم العسكري بأن يحافظ على مبادئ الدستور الأمريكي، والمبادئ العشرة في القانون، لم يكن هذا القسم مجرد قسَم روتيني لإجراء مهمته بل كان يعتبر أن هذا القسم هو «العقد المتوازن بين المواطن والدولة». خدم والد سنودن ثلاثين عامًا في الجيش الأمريكي عبر حراسة السواحل مما عزز شعور سنودن أنّ من واجبه خدمة وطنه، فقال «أردت القتال في العراق لأنني شعرت أن واجبي الإنساني يصبّ في تحرير البشر من الاضطهاد» كان ذلك في مرحلة حكم بوش التي عزز فيها فكرة الحرب من أجل «إنقاذ» الشعب العراقي! فكر سنودن بالالتحاق بالقوات الخاصة،

تقدم لخدمة الجيش وتم قبوله في ربيع 2004 لكن الطريق لم يخلُ من عقبات؛ فسوء نظره واستخدامه للنظارات (6و5 ناقص) وكان أقدامه صغيرة للغاية عرقلت تطوره وجعلت مرحلة الجيش بتدريباتها المركّزة مرحلة في غاية الصعوبة لسنودن، وفي أثناء إحدى تدريبات الاقتحام كسرت كِلا رِجليه، وبعد مرحلة علاجية ليست بقصيرة تم تسريحه من الجيش.

قلة من زملائه في الجيش كانوا يقاسمونه مبادئه «النبيلة» (كما وصفها) حول مساعدة المواطنين المضطهدين وتحريرهم من القيود، فلقد كان زملاؤه - حسب تعبيره - أغلبيتهم «يطوقون لقتل الناس وبالأخص المسلمين، غالبية المدربين بدَوا وكأنهم يريدون فقط قتل العرب ولا يسعون لمساعدة أحد»، عاد بعدها سنودن إلى ميريلاند وشغل وظيفة خبير في الحماية الإلكترونية في المركز التابع للمخابرات العسكرية في الجامعة، «لربما سمح سنودن رغم تاريخه القصير مع الجيش بالاقتراب من هذا العمل الحساس» كان المركز يعمل بشكل وثيق مع المركز الاستخباراتي، لم يكن سنودن يحمل شهادات ذاك الأوان لكنه حصل في منتصف 2006 على وظيفة مبرمج في الـ CIA، مهاراته في مجال الحاسوب فتحت له أبوابا عديدة، بعد فترة قصيرة تم نقل سنودن إلى وزارة الخارجية لخبرته وإمكانياته الإلكترونية العالية، عام 2007 أُرسل سنودن إلى جنيف للقيام بمهمته الأولى خارج الأراضي الأمريكية، كانت مهمته حماية الشبكة الإلكترونية لل- CIA وأجهزة الحاسوب للدبلوماسيين الأمريكيين، كانت هذه التجربة الأولى لـ سنودن خارج أمريكا، جنيف بما تحتويه من أعداد هائلة من أجهزة الاستخبارات والجواسيس العالميين كان نقطة فاصلة في مشوار سنودن. في أكتوبر 2013 نشرت جريدة الشرق الأوسط مقالا ل- ريتشارد كوهين نقلا عن الواشنطن بوست يقول فيه: «بيْد أنني حائر بشأن كيفية التعامل مع سنودن. صحيح أنه خرق القانون، وكان حذرًا في كشف معلوماته، ولكن لا يستطيع معرفة كافة العواقب، وعلى أي حال، لا يمكن للحكومة أن تترك لأي شخص أن يقرر من تلقاء ما يجب الكشف عنه من معلومات، وهذا صحيح أيضًا، إنني أعتقد بضرورة عقاب سنودن، لا أن يُوصم بالخيانة، فربما يكون غير مخلص لأمريكا تقنيًّا لكنه ليس خائنًا للقيم الأمريكية »

الجميع حائرون حول كيفية النظر لما قام به هذا الشاب، هل هو بطل؟هل انتصر للمتجسَّس عليهم وللشعوب المستباحة خصوصيتها؟أم مجرد شخص خان بلده؟كيف ننظر نحن في العالم العربي لسنودن؟وفي المقابل هل ثمّة من يطرح التساؤل؟: من تتجسس علينا؟من تنصّت علينا؟ومن سمع أحاديثنا؟مِن بين الأمور الهامة التي كشف سنودن عنها هي تحالف العيون

الخمس، سوف نحاول فيما يلي أن نقدم بعض المعلومات التي حصلنا عليها حول هذا التحالف، أعتقد أن معرفتنا وفهمنا لوجود تحالفات من هذا النوع تساعدنا في فهم ما نحن بانتظاره هذا القرن.

1.3 تحالف العيون الخمس

لم يكن العالم حتى ظهور سنودن للعلن يعرف ما هو تحالف العيون الخمس، اسم أثار مؤخرًا كثيرًا من التساؤلات حول من يقف خلف تحالف استخباراتي دولي، يشمل دولًا بعينها دون غيرها ويقوم بمهام تجسّسية على البلدان غير المنضوية تحت لواء هذا التحالف. لم يعلن عن ماهية التحالف هذا ذي الشكل الخماسي رسميًّا إلا في شهر يونيو 6 - 2010 حيث تمّ نشر نصّ الاتفاقية الكامل في الأرشيف القومي البريطاني، هذا التحالف المريب هو اتفاق تنضوي تحته دول متحدثة بالإنجليزية هي: بريطانيا وكندا وأستراليا ونيوزيلندا وأمريكا، وهو تحالف تجسّسي استخباراتي تقسِّم فيه البلدان المتحالفة العالم إلى قطاعات مستهدفة بالتصنّت وتتقاسم البلدان الخمسة النتائج، كما ينص الاتفاق على ألا يتصنت أي طرف على الآخر، تأسس الحلف عام 1941 بعد أن نشأ من اتفاقٍ مبدأيٍّ سريٍّ وغير رسميٍّ بين الولايات المتحدة وبريطانيا تم تعديله وتوسيعه وتطويره عام 1946. ولا توجد إلى الآن أي شروحات توضح لماذا تم اختيار هذه البلدان واستثناء أخرى؟منذ تأسيس الحلف إلى أن ظهر سنودن للعلن عام 2012 لم تنشر أو تظهر أية وثيقة أو خبر عن التأسيس أو أعمال هذا التحالف. المفاجأة جاءت للجميع مع بداية التسريبات التي كشفها سنودن، الوثائق التي كشفها سنودن لم تتحدث عن أمور أخرى تخص هذا الحلف سوى التصنت، لم يذكر سنودن أي تفاصيل أخرى تخص نشاطات وحروب قام بها الحلف القرن الماضي أو الآن سوى التجسس. سنودن أطلق شرارة واحدة لا نعلم نحن العامة ما إذا كانت باقي الحقائق ستظهر تباعًا أم أن يكتفي بهذا القدر، بكل الأحوال فإنّ ما كشفه سنودن كان كافيًا ليُقِضّ مضجعَ كثيرٍ من الدول، فحسب سنودن بموجب اتفاقية الحلف بين البلدان الخمس جرى مثلا التصنت على بلدان أوروبية كـ«ألمانيا» تناولته وسائل الإعلام في تاريخ 23 - 10–2013 بصيغة التصنت على هاتف المستشارة الألمانية أنجيلا ميركل، هزّ هذا الخبر عرش السيادة الألمانية وبدأت الأصوات تتعالى حول هذا التحالف لم نكن نسمع عنه اسمه «العيون الخمس»، أثار الخبر الامتعاض لدى عدد من الدول؛ لعدم إشراكها بهذا الحلف. الأمر الذي يعني مباشرة أن هذه الدول عرضة للتجسس في أي وقت من قِبل بلدان الحلف، «فرنسا» كان لها من القلق والامتعاض نصيب، وفق أحد المحللين الأمريكيين فإن «برلين وباريس ترمقهما العاصمتان الحليفتان واشنطن ولندن بعين الحسد»، الحسد هنا لا يخلو من مشاعر خوف حقيقة، كذلك انتابت هذه البلدان وحكوماتها، فبادرت المستشارة الألمانية الحاسدة والخائفة إلى حظر

استخدام أجهزة الهاتف الأيفون من قبل المسؤولين الألمان كإجراء أوّلي، بعد الوثائق التي كشف عنها سنودن بشأن تصنت مزعوم على ميركل، تكهّنت وسائل إعلام ألمانية بأن برلين ربما تسعى للانضمام إلى تحالف التجسس هذا. لكن مسؤول استخبارات أميركا سابقًا قال إنه لكي تدعو ألمانيا للانضمام إلى تلك المجموعة فإنه سيتعين أن يوافق جميع الحلفاء الخمسة، وإن مثل هذه الموافقة غير مرجحة إلى حد بعيد. وتوقع أن تفضي المناقشات الألمانية الأمريكية إلى موافقة واشنطن على عدم التجسس على زعماء ألمان مثل ميركل، وأيضا عدم التصنت على شركات ألمانية لأغراض المنافسة الاقتصادية، واعتبر المسؤول الأمريكي - وفقا لما نقلته رويترز - أن أي وعد من هذا النوع سيكون أجوف، لأن القواعد الأمريكية للتصنت تحظر بالفعل التصنت الرسمي لغرض التجسس الصناعي التجاري، بدوره استبعد مسؤول كبير في إدارة الرئيس الأمريكي باراك أوباما التوصل لاتفاقية عدم تجسس شاملة بين البلدين، أوباما الذي تعرض حينها لسيل من الانتقادات من الخارج؛ فيما يتعلق بأنشطة وكالة الأمن القومي، حاول فرض حظر على التصنت الأمريكي على زعماء الدول المتحالفة مع الولايات المتحدة لكن دون فائدة.

أستراليا المنتمية لهذا الحلف قامت بدور مشابه في إطار هذا التحالف الخماسي وفق سنودن، إذ صرح مسؤولون إندونيسيون أن لديهم شكًّا بأن أجهزة المخابرات الأسترالية (أوزيو) تقوم بمتابعة أجهزة وتليفونات المسؤولين الإندونيسيين بما فيهم رئيس الوزراء وزوجته. إثر هذه الأخبار استدعت وزارة الخارجية الإندونيسية السفير الأسترالي في إندونيسيا لتقديم توضيحات بشأن هذه المسألة)8(وفي هذا الإطار نقلت صحيفة «صنداي مورنينج ذي هيرالد» Sunday morning Herlad The أن المستشار السياسي للرئيس الإندونيسي دانييل سبارنجا ذكر بأن خبر التجسس أرهق الرئيس يودوهيونو خاصة وأنه يسعى دوما لتحسين العلاقات بين البلدين واعتبر أن تعامل السلطات الأسترالية مع الخبر كان مخادعًا؛ حيث صرح ممثل الحكومة الأسترالية أبوت Abbott أن ما فعلته أستراليا لم يكن لإيقاع الأذى؛ وإنما لمساعدة أصدقائنا والحلفاء. الرئيس الإندونيسي استدعى مستشاريه المقربين لبحث المسألة، ومن المسؤولون الذين كانوا عرضة للتجسس؟وما هو الرد المناسب؟، هذا التجسس الذي تقوم به الدول التابعة للحلف الذي أثار امتعاض الكثيرين لأنه طال المسؤولين الكبار ومرافق خاصة وعامة في الدول غير المنضوية تحت لواء الحلف لم يستطع إيجاد اعتذارات رسمية حول هذا الموضوع. كانت هناك دعوات يتيمة لتقديم شروحات واعتذارات لهذه الدول منها جوناثان لورانس (الأستاذ المساعد في العلوم السياسية في بوسطن كوليدج

والمتخصص في العلاقات الأمريكية الألمانية) الذي قال: «إن علينا مسؤولية تقديم اعتذار صادق وطمأنة حقيقية، ولكن لا يمكننا أن نغفل حقيقة أننا لسنا العدو وأن لديهم أعداء. يجب علينا ألا نغفل حقيقة أن الدول الأوروبية ليست تابعة لنا ولكنها بدرجةٍ ما خاضعة لحمايتنا، نحن نوفر مظلة أمن على امتداد العالم ومصالحنا تتداخل كثيراً مع مصالحها». وبالمقابل لم تقم البلدان التي طالها التجسس بأي عمل يذكر سوى الامتعاض والادانة وبعض الإجراءات التقنية بحظر أجهزة الهواتف الذكية عن المسؤولين، ولم يجد الحلف الذي اعتمد السرية في عمله طيلة أكثر من نصف قرن إلا أن يسرّب هو الآخر معلومات بسيطة مثل الإعلان الذي جاء بتاريخ 22 - يناير 2015 حيث أعلن وزير الأمن العام الكندي ستيفن بلاني لتلفزيون سي. تي. في «أن تحالف العيون الخمس سيعقد اجتماعًا لمناقشة مكافحة الإرهاب بعد هجمات باريس، الإعلان جاء مفاجئًا خاصة وأن أعضاء شبكة العيون الخمس نادرا ما يتحدثون عن نشاطهم لكن بدا للجميع أنّ تسريبًا من هذا النوع على ما يبدو، وربطه بالإرهاب سيعطي شرعيةً ما لوجود هذا الحلف.

الوثائق السرية التي سرّبها إدوارد سنودن حول التحالف أظهرت أن التحالف يسعى لاختراق متْجري تطبيقات «جوجل وسامسونغ» بهدف زرع برامج تجسسية في الهواتف الذكية للمستخدمين. وأنّ «فريقا متخصصا بالتصنت الإلكتروني يضم عملاء تحالف «العيون الخمس» ويحمل اسم «فريق تقنيات التجسس الشبكية المتقدمة» عمل على تطوير طرق للسيطرة على خوادم متجر «جوجل بلاي» الذي كان يحمل حينها اسم «أندرويد ماركت» ومتجر سامسونج»، الوثائق نشرتها محطة «سي بي سي نيوز» الكندية بالتعاون مع موقع «ذي إنترسيبت» الإلكتروني المعني بنشر تسريبات سنودن بتاريخ 22 - 5 - 2015، وأظهرت الوثائق أن وكالة الأمن القومي الأمريكية وحلفاءها في «العيون الخمس» كانوا يعملون على سلسلة من التقنيات خلال ورشات عمل عقدت بأستراليا وكندا في الفترة بين نوفمبر/تشرين الثاني 2011 وفبراير/شباط 2012، وأشارت إلى أن التقنيات الأساسية التي تم العمل عليها «كانت تهدف للسيطرة على الاتصالات بين الهواتف ومتاجر التطبيقات من أجل زرع برمجيات خبيثة بالهواتف المستهدفة تفيدهم في أعمال التجسس عن بُعد، وجمع البيانات دون معرفة أصحاب تلك الأجهزة، بحث الفريق كذلك عن إيجاد طريقة للسيطرة الكاملة على خوادم متاجر التطبيقات بشكل يمكنه مستقبلا من توجيه معلومات مغلوطة لا تحمل أي شبهات، لبعض الهواتف المتصلة بهذه المتاجر، ووفق الوثائق؛ فإن الاهتمام بتطوير هذه التقنيات جاء بعد انتشار ثورات الربيع العربي بداية من تونس عام 2010، ولرغبة التحالف الاستخباراتي في الحصول على طرقٍ تقدّمُ له

معلومات مفيدة للتنبؤ بظهور ثورات مماثلة بدول أخرى، خاصة الدول الموجودة بمحيط هذه الثورات؛ حيث سبق وأنْ كشف مستند سرّبه سنودن أنَّ تلك الدول طوّرت - ضمن مشروع آخر - برمجيات خبيثة متعددة للسيطرة والتجسس على الهواتف العاملة بنظام أندرويد و«آي أو إس» وقد رفضت «جوجل» التعليق على تلك التسريبات، كما قالت «سامسونغ» إنها لن تعلّق عليها «في الوقت الحالي» وفقًا لموقع «ذي إنترسيبت».

الفصل الثاني:
أسلحة رقمية وسباق التجسس الرقمي

2.1 البقاء للأقوى رقميًا؟

نعيش حاليًّا في عصر المعلومات والذي يشهد تطورًا سريعًا للتكنولوجيا الرقمية الحديثة، وبفضل هذا التطور الملموس استطعنا الوصول إلى أحدث المعلومات والبيانات؛ لنعبر عن أنفسنا وما يدور حولنا بطرق أكثر ابتكارًا، حتى هذه اللحظة، فإنّ التطورات الحديثة التكنولوجية أدت إلى زيادة قُدرة (الأشخاص، والمجتمعات، والدول والكيانات) لاعتراض، وجمع وتخزين ونشر المعلومات في القطاعين العام والخاص، والتي قد تنتهك حقوق الإنسان الأساسية، وخصوصًا حقنا في الخصوصية، إذًا من المهم معرفة الجوانب والأبعاد القانونية لتلك الخصوصية الفردية من خلال النقاط التالية:

أولاً: - الحقٌّ في الخصوصية هو حقٌّ أساسيٌّ من حقوق الإنسان وهو أمر ضروري لتحقيق العديد من حقوق الإنسان الأخرى، ويعتبر عنصرًا أساسيًّا لمجتمعٍ ديمقراطيٍّ. كما نصت المادة (12) من الإعلان العالمي لحقوق الإنسان (الإعلان العالمي)، والمادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية (العهد الدولي)، على أنه «لا يجوز إخضاع أحد لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، «هذا العهد، وهو معاهدة ملزمة اتفقت عليها (167) دولة، وفي مادة أخرى تنص على أنَّ لكل شخص الحق في حماية القانون من مثل هذه التدخلات أو تلك الحملات «في حين أنّ هذا الحق في الخصوصية ليس مطلقًا، وأي قيود عليه يجب ألا تكون بشكل تعسفي؛ وبالتالي فإنّ تلك القيود يجب أن تكون مدرجة بوضوح في

القانون وأن تكون ردًّا ضروريًّا ومناسبًا للوصول إلى هدف مشروع، على سبيل المثال الأمن القومي.

ثالثًا: في ديسمبر 2013 اعتمدت الجمعية العامة وبدون تصويت القرار (68/167) بشأن الحق في الخصوصية في العصر الرقمي. وفي هذا القرار، أكدت الجمعية العامة للمرة الأولى أن الحقوق المكفولة للناس حاليا يجب أن تكون محمية ومحفوظة (المادة 3)، ودعت جميع الدول إلى الالتزام بواجباتهم في احترام وحماية الحق في الخصوصية والحفاظ على الخصوصية في الاتصالات الرقمية عبر الإنترنت، متضمنًا ذلك مراجعة الإجراءات والممارسات الحالية والتشريعات الوطنية (المادة 4).

نفهم من هذه النقاط الثلاث الواردة في إعلانات الحقوق الأساسية للأفراد (حقوق الإنسان) وبتصويت عام وشامل أنه من الجرائم الكبرى التي ترتقي إلى جرائم الإبادة الجماعية هي السطو والعبث غير الشرعي بالبيانات الشخصية للأفراد وتوزيعها على الجهات المستفيدة مثل الأنظمة القمعية والمؤسسات الاستخباراتية والأمنية وتحالفات ما عبر البحار لغرض إيقاع الأذى المادي والمعنوي على فرد معين أو مجموعة من الأفراد من خلال استخدام تلك المعلومات والبيانات الشخصية في الابتزاز والملاحقة غير القانونية وإسكات الأصوات المناهضة لتلك الحكومات أو الأنظمة والمؤسسات التابعة لها، بالتأكيد سيقول البعض إن تلك الإعلانات والحقوق الأساسية لا تساوي ثمن الحبر الذي كتبت به في ظل الانتهاكات المنهجية والمستمرة لحقوق الإنسان في أرجاء المعمورة. إذًا ما الفائدة من هذا الحق بالخصوصية الرقمية بالأساس إذا كانت الحقوق الأخرى لا وجود لها إلا في مخيلة المواطن المغلوب على أمره؟بالتأكيد أن تلك الإعلانات ووثائق الشرف الحقوقية تعمل كدرعٍ واقٍ في حال تمّ إنشاء وملاحقة بعض الأنشطة والمؤسسات الأمنية في بعض المحاكم التي من الممكن رفع دعاوى قانونية ضد تلك الممارسات وأشباهها، لكن في واقع الأمر أنّ الدول العظمى لا تأبه بالأساس لتلك الدعاوى القانونية حتى وإن كانت تحكم لصالح الأفراد والمؤسسات المتضررة من أعمال القرصنة والتجسس التي تعرضت لها بشكل ممنهج وتحت مسمع ومرأى من السلطات والمنظمات التي تدّعي حماية الحقوق الدستورية للأفراد.

2.2 عيون في السماء

استعرنا اسم هذا الفصل من الكتاب من عنوان لفيلم الأكشن الحربي الأمريكي، الفيلم يحكي قصة استخدام الطائرات المسيّرة في تتبع وقتل الإرهابيين والأفراد الخطرين في القرن الأفريقي وتحديدًا في منطقة الحدود بين كينيا والصومال حيث تنشط حركة الشباب الإسلامية المتطرفة دينيًّا، يقوم سيناريو الفيلم على فكرة الاستخدام المفرط في المراقبة وتحديد الأهداف الخطرة في تلك المنطقة والقصف غير المبرر للمدنيين؛ بحجة ملاحقة العناصر الإرهابية المتطرفة! الفيلم يشدّ المُشاهد لكمية الرصد الرقمي في منطقة معزولة عن العالم حيث مستوى المعيشة للمواطن تحت خط الفقر فما بالنا بما يجري في باقي المناطق! سنأخذ هذا العنوان ونحاول رسم مقاربة أخرى لأنشطة التجسس المختلفة ولكن من زاوية أخرى، إذْ تزودنا خدمة الأقمار الصناعية (satellites) بالكثير من الخدمات لأنشطة الأعمال التجارية المختلفة مثل شركات الشحن لكي تسلك مسارات أقرب وأقل استهلاكًا للطاقة، وتزودنا بالمسارات الجيدة لخرائط جوجل على جوالاتنا وعلى شاشات سياراتنا كل يوم؛ حيث تسهل علينا تلك التنقلات وتشعرنا بِوهْم السيطرة على الطريق، لكن معظم صور الأقمار الصناعية التي نستخدمها يوميًّا هي بالأساس قديمة ويصل عمرها إلى أسابيع أو شهور أو سنوات، وهذا مؤشر أنّ تلك المواقع لم يتم مراقبتها أو أرشفتها رقميًّا من قِبل خدمات الأقمار الصناعية والمسح النهائي!

من المفيد أن نكون قادرين على رؤية صور الأقمار الصناعية في الزمن الحقيقي لمناطق بعينها ولكن تقنيًّا هذا الأمر غير ممكن حاليًّا؛ لأن الأقمار الصناعية في مدار الأرض المنخفض (orbit low earth) لا يمكنها التحليق حول نقطة محددة مثل الطائرات المسيّرة و«الهليكوبتر»؛ لأنها تسير بسرعة مدارية عالية تصل إلى 20 ألف كيلومتر بالساعة؛ لذلك كانت هناك الكثير من الأفكار لنشر أقمار صناعية صغيرة ورخيصة الثمن وبأعداد كبيرة تصل إلى الآلاف ومن السهولة الوصول إلى بيَناتها وصورها على مدار الساعة، من خلال تلك المقاربة قامت الكثير من الشركات مثل شركة (الأرض الآن) الموجودة في بيلفيو في العاصمة واشنطن بالإعلان عن خدمات جديدة لرؤية صور الأقمار الصناعية بالوقت الحقيقي بل وأبعد من ذلك بتزويد بيانات «فيديوية» عن أي مكان في العالم. إنها لفكرة جهنمية تقودنا إلى آفاق أبعد في عالم التجسسية وانتهاك الخصوصية، إنه عصر جديد عنوانه لا مفرّ لك من عيوننا التي تتواجد في كل زاوية من هذا الكوكب! لا ننسى بالطبع أنّ تلك الشركة حصلت على دعم حكومي سخي يقدر بـ- 20 مليون دولارٍ بالإضافة إلى داعمين دوليين منهم شركة «ميكروسوفت» الأمريكية و«سوفت بنك» الياباني بالإضافة إلى عملاق

الدفاع والطيران الأوربي (إيرباص)! من الخدمات التي ستقدمها تلك الشركة لزبائنها المستقبليين هي (تعقب الصيادين غير الشرعيين، مراقبة الأعاصير والهواتف الاستوائية، الكشف عن حرائق الغابات ومناطق البدء فيها، مراقبة البراكين التي تكون على وشك الانفجار، تساعد شركات الإعلام على بناء قصصها الإخبارية، مراقبة حركة الحيتان وطرق هجرتها، مساعدة المدن الذكية؛ لتبقى بكفاءة في خدماتها، المساعدة على مراقبة المزروعات وصحتها، مراقبة مناطق النزاعات الإقليمية والمحلية وتقديم المساعدة الممكنة بالشكل العاجل، بناء نماذج ثلاثية الأبعاد للمدن والقرى حتى في الأماكن البعيدة! وأخيرًا، تمكنك من رؤية منزلك كما يراه رائد الفضاء من خارج الكرة الأرضية الزرقاء.

كل تلك الأمور الإيجابية والرائعة هي مجال ترحيب من قبل كل الأطراف! لكن لنتوقف قليلًا للتفكير حول هذه الإيجابيات هناك ثمن باهظ لكل تلك الخدمات الجليلة والمهمة في حياة أي فرد ومجتمع! ما هو يا تُرى هذا الثمن الباهظ؟إن التصوير بالأقمار الصناعية في الزمن الحقيقي وهو ما يعرف اصطلاحًا ب- (time satellite RTSI imagery - Real) يجعلنا تحت كاميرا عدستها كلما كنا في الخارج نذهب في نزهة أو نقود إلى أماكن عملنا ودراستنا! طبعا سيقول البعض إنّ هذا الأمر فعلا يحصل على هواتفنا الخلوية التي يستطيع أي مزود خدمة في الإنترنت أنْ يصل إليه في حال تم ربط أي هاتف محمول بشبكة الاتصالات أو الإنترنت! حسنا ما هو الجديد في الأمر؟طبعا الأمر يمكن إيقافه في حال أوقفت حقّ الوصول لتلك الخدمات في إعدادات هاتفك الذّكي أو هكذا يدّعون! لكن الأمر مع الأقمار الصناعية وتقنية الـ RTSI مختلف حيث سيتم مراقبتك وأنت تركن سيارتك في موقف «المول التجاري» بالضبط كصورة عين الطائر وبشكل يشبه البث المباشر، وسيكون من السهل تتبعك وأنت في تلك السيارة من أي نقطة وإلى أي هدف أو اتجاه تريده، إذًا هو العبث اللامتناهي في خصوصية الفرد، طبعا سيقول المدافعون إنّ لتلك التقنيات الكثير من الإيجابيات فهي ستسهل عمل رجال الشرطة في مطاردة المشتبه بهم وتتبعهم في الحال ومن موقع الجريمة، ولكن من الممكن استخدام نفس التقنيات في عمليات اغتيال النشطاء والمقاومين والمعارضين والصحفيين الذين يسببون الإزعاج والصداع الدائم للحكومات!

بطبيعة الحال بالنسبة لشركة «الأرض الآن» فإنك ستخسر خصوصيتك للأبد لصالح الخدمات التجارية التي ستقدمها والتي أعلنت عنها في عنوان دعائي عريض هو « في البداية، فإن شركة «الأرض الآن» ستقدم خدمات الفيديو التجارية والرؤية الذكية لمجموعة واسعة من

الحكومات والزبائن الكبار»، من المضحك أيضًا أنّ تلك الشركة تدّعي أنها سوف تغطي كل سنتيمتر من الكرة الأرضية! هل ستسمح حكومة الولايات المتحدة مثلًا بتصوير مواقع سرية حساسة تمسُّ الأمن القومي الأمريكي؟بالطبع لا! «البنتاغون» لن يسمح مطلقًا لأي جهةٍ كانت بالاطلاع على ما تقوم به في المنطقة (51) على سبيل المثال! كما في المثال السابق لشركة «الأرض الآن»، حصل مؤخرًا في فضيحة شركة فيسبوك وعملية تجميع المعلومات لكل المستخدمين وبيعها لطرف ثالث (أي مُشترٍ متحمس لتلك البيانات الهائلة التي تعتبر منجمًا من الذهب والأحجار الكريمة له وحسب أهداف استخدامه لها) كما حصل مع شركة كامبردج أناليتيكا (Cambridge Analytica) حيث كانت تلك الشركة رأس الحربة في جهود انتصار الرئيس الأمريكي دونالد ترامب في حملته الانتخابية لمعركة الرئاسة في سنة 2016 ضد منافسته اللدود هيلاري كلينتون، في كلتا الحالتين لم تكن هناك أي ردة فعل جماهيرية تذكر على هذا الانتهاك الصارخ لمعلومات المستخدمين، إذ لم تختلف ردة الفعل فيما حصل في فضيحة فيسبوك عن تلك التي تخص «الأرض الآن»، لم يمانع أحد أو لم يتحرك أحد! من جهة أخرى هناك الملايين من الناس ممّن يستخدمون المساعد الصوتي من أمازون أليكسا وغيرها من الأجهزة الصوتية المساعدة من مصادر متنوعة وكلها لها القابلية على تسجيل وتخزين المقاطع الصوتية التي ننطقها ونتكلم بها يوميًّا! هل هناك من يتصنت عليها بل وبإمكانه تفعيل خاصية الميكروفون ليتمّ تسجيل كل كلامنا في التوِّ واللحظة وعرضه على المستثمرين القادمين وزبائن متحمسين سماع أصواتنا الجميلة؟

هذا وأعلنت شركة جوجل في تموز عام 2019 «امتعاضها» من تسريب التسجيلات الصوتية لأكثر من آلاف المستهلكين المتكلمين باللغة الفلامية (هي إحدى اللغات الأوربية النادرة والتي يتكلم بها قلة من سكان غرب ألمانيا وسكان هولندا وبلجيكا وللوكسمبورغ) وكان الزبون هنا هو: إحدى المؤسسات الصحفية في بلجيكا التي لم تفصح جوجل عنه! بالتأكيد فتلك الممارسة هي معروفة على نطاق واسع من خلال جمع الشركات التقنية كل التسجيلات الصوتية لمجموعة من الناطقين باللغات المختلفة لاستخدام تلك البيانات الصوتية في تدريب شبكات الذكاء الاصطناعي المسؤولة عن تلك المساعدات الصوتية من خلال برامج معالجة اللغات الطبيعية (language processing Natural NLP) وبرامج ترميز المؤشرات الصوتية البشرية!

طبعا لا يقف الأمر عند هذه الشركات وقصصها المنتشرة يوميًّا بل حتى الشركات الصغيرة التي تصنع منتجات رقمية تسمى بال- (gadgets) منها ساعات مراقبة الصحة واللياقة البدنية والمساعدات الصوتية الموجودة في السيارات وكاميرات المراقبة الصغيرة التي تركب في السيارات لمراقبة الطريق وأرشفة الحوادث ومنها ألعاب الأطفال الرقمية مثل الروبوتات الصغيرة الحجم والتي تساعد في الأعمال المنزلية المتعددة وأنظمة إنترنت الأشياء. بالتأكيد لن تمانع الأغلبية من الناس حول تلك النقطة بالذات؛ لأنّ الخدماتِ المقابلة انتهاك خصوصيتهم مغرية بالفعل؛ لأننا رضينا بصورة كبيرة عن تلك الخدمات مقابل التضحية المُرة بأدقّ خصوصيات حياتنا فأين المشكلة بالأساس؟في الواقع لا توجد مشكلة لأننا لن نمانع أبدًا، لأننا نحب أن نبقى متصلين بالإنترنت مع أفراد العائلة والأصدقاء وأن نعمل على تكوين صداقات جديدة، وأن تبقى هواتفنا الذكيّة تعمل على مدار الساعة وتقودنا إلى المطاعم الأكثر شعبية في أطباقها وإلى أماكن النزهة والمرح وأن تعطينا تلك الخدمات التوصية لأفضل الأفلام والمسلسلات بناء على تاريخ مشاهداتنا المستمرة.

إذًا ما المشكلة إنْ تلصّصت تلك الخدمات علينا وعلى حياتنا؟أصبحت تلك القناعات الصغيرة مزروعة داخل وعْينا سواء اعترضنا عليها قليلًا أم لا، بالنظر إلى كل ما يحصل حولنا وتحت رعاية قانونية حكومية والتي بدأت بزرع كاميرات المراقبة في كل شارع وزقاق لحمايتنا من الجريمة وتبعاتها! كلها قد تم قبولها وبكل ممنونية ودون أدنى اعتراض فما الفرق إذًا بينها وبين شركة «الأرض الآن» وخدماتها المستقبلية؟أو المساعدات الصوتية لشركة «أمازون وأبل وجوجل» أو الساعات الذكية وأساور اللياقة البدنية طالما أننا متراضون بما تقدّم لنا من خدمات ورفاهية كنا نحلم بها قبل عشر سنوات مثلًا؟هنا المشكلة التي لم نفطن إليها وهي حب الشهوة الجامحة لدى بني البشر، حب الاستحواذ على الخدمات والظهور بمظهر الترف والغنى والطمع بخدمات أخرى تشبع تلك الرغبات الدفينة! إنه التلاعب الذكي بسيكولوجيا الدماغ البشري وفك ألغازها يومًا بعد يوم بطريقة تشبه كُرات الثلج التي تكبر وتكبر كلما تقدمت في طريقها نحو المنحدر! إنما إلى أين؟لا أحد يعلم بالضبط!

2.3 المواطن المدجن ونظام النقاط

«إنه سلاح جديد لتدجين المواطن بحيث
يصبح جزءًا من اللعبة لا ضدها»

- راشيل بوتسمان

كلما تقدم الزمن أصبحت حياتنا كتابًا مفتوحًا للجميع وبشكل متسارع، سنشارك الكثير من معلوماتنا الشخصية وسوف يقوم الآخرون بذلك أيضًا، هذا هو الحال في العالم الافتراضي لكن في الحياة «الحقيقية» ثمّة تغيرات مخيفة، فعلى مدار الأشهر الثلاثة الأولى من عام 2017 بدتِ الأحوال طبيعية كعادتها في مدينة «شينزن» الحضرية جنوب الصين، أحوال اعتادها أهالي المدينة وحتى المدن المجاورة التي تحظى بالروتين اليومي نفسه تقريبًا، ومشاهدُ تقليدية لسكان «شينزن» بينها الوجود اليومي تقريبا لخبراءَ تقنيين يضعون كاميرات وشاشات كبيرة فوق إشارات المرور، ومن ثم يقومون بتوصيل كل مجموعة على صندوق أسود مُثبّت على عمود حديدي على جانب كل طريق، ولم يكن مشهد الشاشات بعد عملها بمرور الأيام مستهجنًا بحال وهي تعرِض صورًا مختلفة تخاطب الناس في الشوارع بشكل مستمر، إلا أنّ «غان ليبنج»، الفتاة الصينية الواصلة منتصف العام نفسِه من الأرياف النائية الفقيرة في الصين في مقاطعة «شينزن»، سرعان ما أثارت تلك الشاشاتُ الكبيرة واللامعة فضولها وربما خوفها أيضًا، خاصة وهي ترى عرضا مستمرًّا طوال اليوم للمعلومات والبيانات الشخصية للكثير من المارة، مع تلفظ تلك الشاشات لأسمائهم و«جريمتهم» الحالية وسوابقهم بمجرد مخالفتهم لأي قاعدة مرورية، لتقودَها التجربة المفاجئة في إحدى ليالي نوفمبر/تشرين الثاني من العام نفسه لمعرفة وظيفتها بأوضح وسيلة ممكنة (المصدر: مجلة ميدان باللغة العربية)، لم تكن «ليبنج» أمام أحد أفلام الخيال العلمي، أو تلعبُ دور «وينستون» مع شاشات الرصد في مسرحية تحاكي فصلًا من رواية «1984» الشهيرة لجورج أورويل، وكل ما تطلبه الأمر منها تكرار لخطأ مشاة فقط، فعندما وصلت بدراجتها لعبور الطريق كما أخبرت صحيفة «وول ستريت جورنال»، سارعت للرصيف الآخر محاولة تفادي انتهاء زمن العبور، إلا أن الإضاءة الحمراء كانت بمنزلة تأكيد سريع على أنها فشَلت في ذلك، ولأن تلك هي المخالفة الثانية لـ «ليبنج»، كان النظام بالفعل يتعرف على وجهها ليضعها على شاشات الطريق معلنًا أنها «صاحبةُ جناية مكررة».

هذا عن الصين، أما الولايات المتحدة، فقد عرضت مسلسلًا شهيرًا يُدعى «المرايا السوداء». الذي اعتبر لاحقا من أهم الأعمال الدرامية التلفزيونية التي تستشفي المستقبل القريب، ففي إحدى حلقات هذا المسلسل المحاكي للواقع والمستقبل المنظور بعنوان (nosedive) أو الانحدار، سنجد فتاة تعيش في عصر يعتمد على نظام النقاط التي تحدد مستوى الفرد من الناحية الشخصية والاجتماعية والاقتصادية حتى في شكل يقترب حاليا منه بعض الشيء نظام المستوى الائتماني (credit history) المعمول به في العالم الغربي وخاصة أمريكا الشمالية والذي يتم تقييم القدرة المالية والائتمانية للفرد من خلال عمليات الإنفاق والاقتراض التي يقوم بها! يقوم الناس هنا بعملية التقييم العام للشخص معتمدا على الكيمياء الشخصية للفرد وهو أسلوب رديء لا يمكن تمييزه عن التحيز البنيوي لشعور الإنسان الكاذب تجاه المؤثرات الفيزيائية والكيميائية المختلفة من شخص لآخر؛ ولذلك تمر الفتاة بالعديد من المشاكل والاهتزازات النفسية؛ لأنها لم يكن باستطاعتها جمع النقاط الكافية للذهاب إلى الحفلات الراقية التي تمكنها من رفع مستواها الاجتماعي! ولذلك فإن نظام النقاط يعتبر من أسوأ الأنظمة الاجتماعية التي طبقها الجنس البشري لأنه يكرّس للتمييز الطبقي والاجتماعي بشكل صارخ وعشوائي. النظام هذا الذي تصوره الحلقة التلفزيونية هو ذاته نظام النقاط الذي قامت الحكومة الصينية بتطبيقه إذ يتم فرض عقوبات على المواطنين الذين حصلوا على عدد نقاط قليلة أي (score citizens low) حيث أحصت ما يقارب التسعة ملايين مواطن صنفوا ضمن هذه الفئة غير المحظوظة! ومنعتهم من شراء تذاكر القطارات أو الطيران حسب ما صرحت به الإحصاءات الصينية الرسمية! وهنا يجب أن نفهم تلك الميكانيكية الجرمية التي تعتمدها السلطات هناك لتمنع مواطنيها من أحد الحقوق الأساسية للإنسان وهي حق السفر والتنقل بُحرية، وفي بعض الأحيان ينتقل نظام العقوبات هذا إلى مستوى آخر وهي منع حتى من لديهم نقاط عالية من شراء تذاكر الدرجة الأولى ودرجة رجال الأعمال، طبعا كيف يمكن للسلطات السيطرة على تلك الأعداد الهائلة من المسافرين والذين يصلون إلى ملايين الأشخاص في السنة الواحدة تقريبًا في مطار شنغهاي لوحده! ربما يبدو سؤالا غبيًّا لكنه مقصود!؛ لأن بيانات الشعب الصيني كلها بيَدِ جهة مركزية واحدة هي تسمع وترى وتراقب كل شاردة وواردة. العقوبات لم تقتصر على شراء التذاكر بل تعداها إلى العقوبات الجماعية للعوائل التي لا تجمع نقاط معينة في هذا النظام بل ويمكن أن تحرم العائلة من أن يرتاد أطفالها المدارس الحكومية الجيدة. حدث ذلك في تموز الماضي حين منعت إحدى المدارس الصينية أحد الطلبة من

التسجيل بها؛ بحجة أن والد الطالب له تصنيف اجتماعي رديء (bad social score)، هنا طبعًا نرى اختفاء الموديل الشيوعي للمساواة الاقتصادية واقتصاره على تعميم موديل الأخ الأكبر (Big brother)، وبتمثيل ذلك على نطاق أوسع وتشمل العقوبات مثلًا بعض القرى والمدن التي تفشل في جمع نقاطها أو خرق بعض القوانين التي تؤدي إلى تخفيض نقاطها، فهل يؤدي ذلك إلى انهيار اجتماعي بسبب هذا النظام غير العادل؟هذا السؤال أجابت عليه أحد أكبر المختصّين بالأمن الرقمي راشيل بوتسمان Rachel Botsman التي نشرت كتابها حول عمليات التجسس التي تقوم بها الدول على نطاق وطني وإقليمي! كانت إجابتها إنه سلاح جديد لتدجين المواطن بحيث يصبح جزءًا من اللعبة لا ضدها ومن خلال المتاهات المتشابكة من العقوبات والجوائز أيضًا ستقوم الحكومة بالسيطرة الكاملة على مواطنيها داخل حدودها الإقليمية وربما إلى ما بعدها! وهذا ما رأيناه ماثلًا أمامنا في الاحتجاجات الأخيرة في هونغ كونغ حيث انتفض المواطنون ضد قانون الجرائم الذي أقرته الحكومة المحلية بالضغط من قبل الحكومة المركزية في بكين، وهنا استغلت تلك الأحداث الدوائر الغربية لإحداث أزمات مفتعلة ضد الصين، فهنا أصبحت عمليات المراقبة أحد الأسلحة الاستراتيجية التي يمكن أنْ تحدث فرقًا كبيرًا في موازين أي مواجهة محتملة مع الأطراف المتصارعة.

إنّ هذا النظام المرعب ربما سيكون محفزًا للدول الأخرى لتحذو حذوَهُ وكل ما تحتاجه هو منظومة مراقبة وتسجيل تعمل على نطاق واسع مرتبطة بشبكات تراكبية ومعقدة لتتمكن من رصد أي عنصر (element) يقوم بأعمال تخفض من نقاطه الاجتماعية فيصبح الكل سجناء داخل تلك النقاط! إنه رعب حقيقي قادم إلينا لا محالة فلا حقوق شخصية ومِن ثَم تدخُّل الحكومة حتى في علاقتك الحميمية على الفراش! بالطبع فإنه زاوية انتهاك الخصوصية في هذا الأمر بالذات يبعث على الريبة على المستوى الفردي، ولكن هل كل الناس يأبهون لهذا الأمر؟أو هل يمكن أن تكون انتهاك الخصوصية شيئا يبعث على القلق لدى كل الأفراد؟

2.4الهوية البيومترية وأحصنة طروادة

من بديهيات التعريف الشخصي في القرن الحالي هو استخدام بطاقة الهوية وكلمة المرور وتعتبر هذه البطاقة من الأدوات التي نحتاجها للقيام بمهمات بسيطة في حياتنا لكن، ونظرًا لكون هذه البطاقات البسيطة ضعيفة فهي عرضة للاستغلال والاحتيال؛ تحت هذه الذريعة القابلة للتصديق تَم تطوير تقنيات القياس الحيوي physiological measurement systems. هذه القياسات الحيوية هي الخصائص الفسيولوجية أو السلوكية المستخرجة من الموضوعات البشرية، مثل بصمات الأصابع وقزحية العين والوجه والصوت والقلب، وتستخدم للتعرّف على الهوية والتحقق منها، باستخدام القياسات الحيوية، من الممكن تأكيد أو تحديد هوية الفرد بناءً على «مَنْ هو»، بدلاً مِن «ما هو / هي» (مثل بطاقة الهوية) أو «ما يتذكره» (على سبيل المثال، كلمة المرور). نظام المقاييس الحيوية هو النظام الذي يتم فيه تحديد هوية الشخص عن طريق خصائصه المميزة أو النوعية أساسًا للشخص الذي ينتمي إلى شخص ما، لا يوفر التعرف على البشر الذين يستخدمون أجهزة الكمبيوتر بعضًا من أفضل الحلول الأمنية فحسب، بل يساعد أيضًا على تقديم الخدمات البشرية بكفاءة. يربط نظام التوثيق الحيوي السمات السلوكية أو الفسيولوجية لتحديد هوية الشخص أو التحقق منه. تعتمد الشخصيات الفسيولوجية على السمات الجسدية، مثل بصمة الإصبع وقزحية العين وهيكل الوجه، إلخ. تستند السمات السلوكية إلى الخصائص السلوكية الفريدة للفرد، مثل الصوت والتوقيع وما إلى ذلك.

في السنوات الأخيرة، أصبح من المهم للغاية تحديد هوية المستخدم في الكثير من تطبيقات الحياة المختلفة في أوروبا وأمريكا وأنحاء مختلفة من العالم. وهذا في مجالات مثل أمن الأفراد والدفاع والمالية والمطار والمستشفى والعديد من المجالات الهامة الأخرى؛ لذلك، أصبح إلزاميًّا استخدام نظام مصادقة الهوية الشخصية والتحديد القوي والموثوق به لتحديد هوية ذلك المستخدم، في وقتٍ سابقٍ كانت طرق تحديد هوية المستخدم تعتمد بشكل أساسي على المعرفة مثل كلمة مرور المستخدم أو حيازة بوابة عبور فيزيائية مثل مفتاح المستخدم أو الـ dongle؛ ولكن نظرًا لضعف هذه الأساليب، كان من السهل على الأشخاص صياغة المعلومات. وبالتالي، فإن أنظمة القياس الحيوي التي تعتمد على الأداء الحسابي لتحديد الهوية، حيث يتم التعرف على المستخدم باستخدام

القياسات الحيوية الخاصة به. تستخدم القياسات الحيوية طرقًا للتعرف على المستخدمين بناءً على واحدة أو أكثر من السمات الجسدية والسلوكية. وبالتالي، أصبحت أنظمة تحديد الهوية التقليدية مثل القزحية وبصمات الأصابع والوجه والكلام شائعة في تحديد هوية المستخدم والتحقق منه.

كيف يمكن توظيف هذه المعلومات عسكريًّا؟كيف سوف تستغل هذه المعلومات؟لنرى ما يلي، قبل ضغط الزناد، يجب أن يكون القناص الذي يخطط لاغتيال أحد عناصر العدو متأكدًا من وجود الشخص المناسب في الشعرات المتقاطعة في منظاره. تستخدم القوات الغربية عادةً برامج تقارن بين ملامح وجه المشتبه فيه أو المشية مع تلك المسجلة في مكتبات البيانات الحيوية التي جمعتها الشرطة ووكالات الاستخبارات، ومع ذلك، يمكن إحباط هذه التكنولوجيا من خلال غطاء أو غطاء للرأس أو حتى عثرة متأثرة؛ لهذا السبب، كانت قيادة العمليات الخاصة الأمريكية (SOC)، التي تشرف على الوحدات المسؤولة عن هذه العمليات في مختلف أذرع القوّات الأمريكية المسلحة، تريد وبإصرار منذ فترة طويلة طرقًا إضافية لتأكيد هوية الهدف المحتمل استجابة لطلب من العمليات الخاصة، طوّر مكتب الدعم الفني لمكافحة الإرهاب (CTTSO)، إحدى وكالات وزارة الدفاع، أداة جديدة لهذا الهدف التقني، تلك الأداة هي خاصية التأكيد البارومتري عن طريق ضربات القلب أو التخطيط الصوتي للقلب (phonocardiography signal processing). هذا النظام، المسمى Jetson، قادر على قياس ضربات القلب الميكانيكية، من مسافة تصل إلى200 متر، من خلال جسّ الاهتزازات التي تحدثها الملابس من قبل نبضات القلب لشخص ما، نظرًا لاختلاف القلوب من حيث الشكل ونمط الانكماش، تختلف تفاصيل نبضات القلب أيضًا.

الفصل الثالث

جدران ذكية

3.1 إنترنت الأشياء

«إنترنت الأشياء هو حصان طروادة الجديد
في حياتنا الشخصية»

- المؤلفين

لعل الأمر كما نتصوره سوف يصبح خلال بضعة سنوات لا أكثر، أكبر من مجرد حصان طروادة الإغريقي الذي يقتحم حياتنا مدجّجًا بالمقاتلين والعتاد، لكن الدهشة سوف تكون حينها حين نعلم أن المقاتلين لم يصلوا عقر دارنا وحسب بل إنهم وصلوا إلى غرفة النوم بل وإلى كل زوايا البيت، لكننا لم نخدع قط هذه المرة! الاقتحام جاء بكامل إرادتنا ورغبتنا! فنحن نستيقظ على صوت المنبهات الرقمية أو الهاتف الذكي وبعدها يقوم المنبه بتوجيهنا إلى أخذ حمام صباحي وغسل أسناننا ومراقبة الإشارات الفسيولوجية والتأكد من صحة الإدرار وإفرازات أجسامنا الأخرى، وبعد ذلك يظهر لنا على المرآة الذكية الجدول اليومي الذي ينتظرنا سواء كان لغرض المتعة أو العمل أو للعائلة أو غير ذلك، بعدها نذهب إلى الثلاجة وهناك توصلنا الشاشة التي تعمل باللمس أو بالأوامر الصوتية إلى وجبة الفطور ومكوناتها وتنصحنا باختيار الطبق الأفضل ويتم تسخين الأكل وتحضيره حسب الأوامر التي أعدتها ثلاجة المطبخ ومن هنا يبدو وكأنّ الحياة بدت سهلة وأنّ كل شيء بات مؤتمنًا عليه، بل وقابل للسيطرة عليه من خلال أجهزة متصلة بالإنترنت سواء كانت أجهزة منزلية أو سخان كهربائي أو حتى باب المنزل والشبابيك وأنظمة التكييف والتبريد وحتى أنظمة السيطرة على استهلاك الطاقة الكهربائية. الاتصال

بالإنترنت سوف يكون متاحًا لكل جهاز موجود داخل وخارج منزلك وكل تقنية يمكنك استخدامها يوميا لتسهيل حياتك ومعيشتك! هناك غالبية عظمى ترى في ذلك تقدمًا للبشرية لم يسبق له مثيل ولذلك ليس هناك أي قلق على احتمالية أن تكون تلك الأجهزة قاعدة تجسس لأفراد آخرين يقبعون خلف شاشة أخرى تراقبك باستمرار وتتعمد التلصّص عليك بشكل يومي ليلًا ونهارًا.

لكن مهلًا قليلًا فمن يدري مَن الذي يجلس خلف شاشته؟وما الذي يجري في دهاليز مؤسسات تجسس سواء كانت شركة أو حكومة أو منظمة إجرامية أو غير ذلك؟الخبر السيئ هو أن كل الأجهزة المرتبطة بالإنترنت داخل المنزل تعمل بشكل متناسق وكل البيانات التي تعالج بها ينتهي بها الأمر في خوادم الشركة المجهزة لتلك التقنيات المنزلية. هذا ناهيك عن معضلة الجدران الذكية التي تحيط بنا من كل جانب، حيث أظهرت الكثير من الأبحاث عمليات رصد التطورات التي صاحبت التقنيات المنزلية والمرتبطة بمنظومات ما يسمى بـ إنترنت الأشياء والأخير هو عبارة عن مجموعة التقنيات التي ترتبط بالإنترنت سواء كانت منزلية كهربائية ميكانيكية الكهروميكانيكي حرارية أو الروبوتات مساعدة أو منبهات رقمية، فكل تلك الأجهزة مليئة بالمجسات والمتحسسات (sensors and transducers) الفيزيائية مثل الميكرفون وسماعات وكاميرات مراقبة وكل تلك المتحسسات قابلة للاختراق سواء شئنا أم أبينا وعلى مدار الساعة طالما هي متصلة بالإنترنت ويتم تزويدها بالتيار الكهربائي أو الطاقة. بالطبع يردد بعض الخبراء من البيانات التي يتم جمعها من قِبل تلك الأجهزة المنزلية والمرتبطة بالإنترنت ستوضع لاحقًا في خوادم معينة تتبع للشركة المصنعة لها وهذا لا شكّ فيه أمر مفروغ منه بالإضافة إلى ذلك فإنه تلك البيانات تخضع للتشفير ما يجعلها محمية غالبا برموز من الصعب كسرها أي بمعنى أن البيانات لا يمكن رؤيتها إلّا من قِبل طرف الشركة المجهّزة أو مِن طرف المستخدم أو من قبل، إلا أن هناك أمراً مُهمًّا قد تم إهماله وهو حول إمكانية وجود طرف ثالث ساهم بتصنيع تلك الأجهزة من خلال شرائح إلكترونية أو من خلال متحسسات ذكية في داخلها شرائح حاسوبية صغيرة؟. يجب توجيه هذا السؤال بطبيعة الحال إلى الشركة المصنعة في تلك الأجزاء حول علاقتها بالشركات الأخرى أو ما يسمى بالطرف الثالث أو المجهز الثالث. وهنا تأتي الحسابات التجارية فهناك بعض مستأجري أو مجهزي الشرائح الإلكترونية الذكية قد يعمد إلى تفعيل خاصية التصنت والتجسس في أجهزتهم من خلال تشغيل المجسمات الميكروفون والكاميرات وحتى متحسس درجات الحرارة والرطوبة، وقد يتم هذا التفعيل

حتى من دون علم الشركة المُصدّرة وهنا تكمن المشكلة حول الشركة المصنعة ومسؤوليتها الأخلاقية عن فعل التجسس الذي يقوم به الطرف الثالث!

يفتح العدد المتزايد من الأجهزة المتصلة بالإنترنت المؤسسات أمام ثغرات أمنية إضافية في الإنترنت. ومع ذلك، يقول ما يقرب من نصف صنّاع القرار في تكنولوجيا المعلومات وصناع القرار في مجال الأمن: أنّ الأمن السيبراني هو فكرة لاحقة عند تنفيذ المزيد من أجهزة إنترنت الأشياء (IoT) في شبكات الشركات. فوفقًا لـ IoT Analytics، سيزداد عدد أجهزة IoT المثبتة من 7 مليارات تقريبًا اليوم إلى أكثر من 21 مليار بحلول عام 2025. وستزداد فرص مختلف الأطراف لإحداث خروقات للبيانات بسبب المزيد من الثغرات الأمنية. تشمل أمثلة أجهزة إنترنت الأشياء:

- المستهلك: منظمات الحرارة، أنظمة المنزل الذكي، الكاميرات، الأجهزة، السيارات.
- الأعمال: أجهزة استشعار التحكم في العمليات، مكونات البنية التحتية للحوسبة، أنظمة الوصول الفعلي، الكاميرات.
- الحكومة: الكاميرات، ومراقبة الحركة، وأجهزة استشعار مراقبة البنية التحتية.

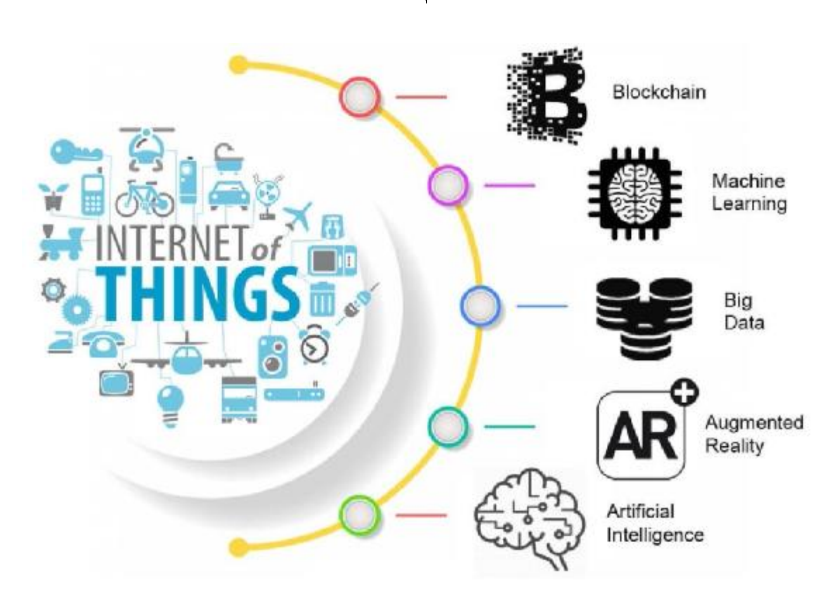
يمكن أن تكون أجهزة إنترنت الأشياء محفوفة بالمخاطر بشكل خاص لأنها تجلس عادةً حيث يلتقي العالم الرقمي بالعالم المادي. نتيجة لذلك؛ قد يكون لاختراق أجهزة إنترنت الأشياء عواقب وخيمة على العالم الحقيقي. تشمل أمثلة اختراق البنية الأساسية محطات توليد الكهرباء الضارة ومحطات معالجة المياه ومصافي النفط والغاز والسكك الحديدية. النتائج الرئيسية لخرق بيانات إنترنت الأشياء هي:

- فقدان ثقة العميل مما يؤدي إلى فقدان السُّمعة والمبيعات والحسابات المغلقة.
- الخسارة المالية الناجمة عن دفع الفدية.
- التكلفة المالية لاستعادة التشغيل العادي بعد توقف حريق أو انفجار أو تصنيع لفقدان استمرارية العمل مما يؤدي إلى الإفلاس.

- التكلفة المالية للغرامات المفروضة من قبل المنظمين عن انتهاكات خصوصية البيانات.

وللتوضيح أكثر عن إنترنت الأشياء بنظرة مختصرة فنقول ما يلي إنترنت الأشياء Internet of Things (IoT) هو: عبارة عن اتصال مستمر بالكائنات (المكونات) المادية مثل الأجهزة والمركبات والمباني والعناصر الأخرى المضمنة مع الإلكترونيات والبرامج وأجهزة الاستشعار واتصال الشبكات التي تمكن هذه الكائنات الفيزيائية من جمع البيانات وتبادلها، يشير «شيء» إلى جهاز متصل بالإنترنت وينقل معلومات الجهاز إلى أجهزة أخرى. هناك اتجاه مثير للاهتمام يساهم في نمو إنترنت الأشياء وهو التحول من الإنترنت IPv4 المستند إلى المستهلك من الأجهزة اللوحية وأجهزة الكمبيوتر المحمولة، أي تقنية المعلومات (IT)، إلى تفاعلات IPv6 المستندة إلى تقنية التشغيل (OT). يتضمن ذلك المستشعرات والكائنات الذكية والأنظمة المجمعة (على سبيل المثال، الشبكة الذكية). يعد الإنترنت IPv6 أحد أهم وسائل الاتصال في إنترنت الأشياء، حيث لا يمكن إضافة مليارات الأجهزة إلى الإنترنت IPv4. يقوم إنترنت الأشياء بتحويل نماذج الأعمال من خلال مساعدة الشركات على الانتقال من صناعة المنتجات والخدمات ببساطة إلى الشركات التي تعطي عملائها النتائج المرجوة بشكل سريع، من خلال التأثير على نماذج أعمال المؤسسات، فإن الجمع بين الأجهزة وأجهزة الاستشعار التي تدعم تقنية إنترنت الأشياء والتعلم الآلي يخلق عالماً تعاونيًا ومترابطًا يربط نفسه بالنتائج والابتكار بحيث يمكن للشركات الآن جمع البيانات وتحويلها إلى معلومات قابلة للاستخدام وقيمة مع إنترنت الأشياء، رغم أن النموذج العمودي من الذكاء الاصطناعي ما زال محوريًّا، إلا أن ضجيجه لا يزال قائمًا، حيث يمكن القول إن كمية التضخيم المحيطة بالذكاء الاصطناعي (Artificial intelligence) في الأمن السيبراني بدأت في الانحسار، لكننا لا نتوقع أن يتحسن الموقف بشكل كبير؛ حيث يتم استخدام مصطلح «AI» على كل الأشياء، والكثير منها مجرد أشجار قرار (Decision - tree) أو خوارزميات أو برامج. هذا لا يعني أن الذكاء الاصطناعي ليس لديه إمكانات هائلة، بالطبع، لكن المصطلح الفعلي «AI» حقق نوعًا من المظلة لا يعني شيئًا على وجه الخصوص، نقدم هنا مثالًا حيًّا لإحدى النقاشات المحتدمة «كان هناك اجتماع مع عدد كبير من قادة الأمن السيبراني وكان الموضوع يدور حول كيفية قيام الذكاء الاصطناعي بتحفيز التغيير في السلوك.» يتذكر أحد الخبراء مداخلته «بعد مداخلات عديدة رفعت يدي وقلت: لم يصف أحد حالة الاستخدام الذكي المصطنع، يا رفاق، فقط تصف سير عمل العملية والبرامج. إذا لم يكن هناك شيء يشبه نموذج التعلم الآلي أو قدرة الشبكات العصبية وراء

الكواليس، فهو مجرد برنامج، ونظرًا لأنّ المؤسسات تطبق مبادئ التحول الرقمي على أعمالها بشكل روتيني، فإن الجمع بين إنترنت الأشياء والذكاء الاصطناعي يمكن أن يخلق اضطرابًا في صناعتها قد لا تكون مستعدة لتداعياته. سواءً كانت المنظمة أو الشركات تستخدم IoT وAI لإشراك العملاء، أو تنفيذ خطط لمحادثة للعملاء على تلك الرؤى التطويرية، أو تخصيص تجارب المستخدم، أو الحصول على التحليلات المناسبة، أو تحسين الإنتاجية من خلال الرؤى والتنبؤات التي يقدمها الذكاء الاصطناعي (AI)؛ ولهذا السبب فإن استخدام IoT وAI يخلق ديناميكية وحيوية كبيرة حيث تكون الشركات قادرة على الحصول على جودة عالية ذات نظرة ثاقبة ودقيقة على كل جزء من تلك البيانات، مما يبحث عنه العملاء فعليًّا ويتطرق إلى كيفية تفاعل الموظفين والموردين والشركاء مع جوانب مختلفة من النظام البيئي. بدلًا من مجرد وضع العمليات التجارية على غرار البرامج بطريقة تقارب العالم الحقيقي، توفر أجهزة إنترنت الأشياء الأنظمة واجهة فعلية للعالم الحقيقي. في أي مكان يمكنك وضع جهاز استشعار فيه أو جهاز لقياس أو التفاعل أو تحليل شيء ما، يمكنك توصيل جهاز إنترنت الأشياء بسحابة تدعم AI لإضافة كميات كبيرة من القيمة.



شكل (1) مخطط لما سيشهده قطاع إنترنت الأشياء بعد دمج العديد من التطبيقات الخاصة بالبيانات الضخمة وتعلّم الآلة والذكاء الاصطناعي والواقع المعزز وغيرها من التطورات التقنية المتسارعة في شتى المجالات (المصدر: Iwaytrack)

إنّ التحديات الشائعة التي تواجهها المنظمات اليوم مع الذكاء الاصطناعي وإنترنت الأشياء هي مع تطبيق وإمكانية الوصول وتحليل بيانات إنترنت الأشياء. إذا كان لديك مجموعة من البيانات

من مصادر مختلفة، يمكنك إجراء بعض التحليل الإحصائي (statistical analysis) باستخدام هذه البيانات. ولكن، إذا كنت تريد أن تكون استباقي في توقع الأحداث لاتخاذ إجراءات مستقبلية وفقًا لذلك، مثل متى يتم تغيير أداة الحفر أو توقع حدوث عطل في إحدى الآليات، فيجب على الشركة أن تتعلم كيفية استخدام هذه التقنيات لتطبيقها على التمييز الفعال على هذا النوع من البيانات العملياتية. وهنا بالتأكيد سيكون لاختراق تلك البيانات هو ما يسيل له لعاب الكثير من الأطراف؛ لأنها تحوي كنوزًا كبيرة من المعلومات والتي لا يمكن الحصول عليها بالطرق الاعتيادية. تعتبر الكمية الهائلة لبيانات إنترنت الأشياء، لا سيما في المنظمات التي نشرت أجهزة استشعار أو علامات وصولاً إلى مستوى الوحدة الفردية مهمة. من الصعب للغاية إدارة الكم الهائل من البيانات المتغيرة باستمرار باستخدام أدوات تحليلات الأعمال التقليدية. هذا هو المكان الذي تدخل فيه الذكاء الاصطناعي. من خلال استخدام أساليب التعلم والتجميع غير الخاضعة للرقابة، يمكن لأنظمة التعلم الآلي تحديد الأنماط العادية وغير الطبيعية في البيانات وتنبيههم عندما تنحرف الأشياء عن المعايير المرصودة، دون الحاجة إلى الإعداد المسبق من قبل المشغلين البشريين. وبالمثل، يمكن لأنظمة IoT المدعومة من الذكاء الاصطناعي أن تبرز الرؤى ذات الصلة تلقائيًا والتي قد لا تكون مرئية مثل كومة قش من البيانات التي تجعل تلك الرؤى غير مرئية تقريبًا. تقوم الشركات بتنفيذ أنظمة إنترنت الأشياء التي تدعم الذكاء الاصطناعي AI بعدد من الطرق المختلفة. تقوم شركات الحلول بإنتاج رموز وقوالب جاهزة مسبقًا تشتمل على نماذج مجربة ومختبرة لنطاقات تطبيقية معينة مثل النقل البحري واللوجستيات والتصنيع والطاقة والبيئة وعمليات البناء والمرافق ونماذج أخرى. يقوم الآخرون بإنشاء حلول للعملاء، بناء نماذجهم الخاصة وتدريبهم، مع الاستفادة من مقدّمي الخدمات السحابية لتسخير طاقة وحدة المعالجة المركزية الخارجية. تقوم بعض الحلول بتركيز إمكانات الذكاء الاصطناعي في الحلول الداخلية أو العروض المستندة إلى مجموعة النظراء العملياتية، بينما تهدف الحلول الأخرى إلى تحقيق اللامركزية في قدرات الذكاء الاصطناعي، ودفع نماذج تعلم الآلة إلى الحافة للحفاظ على البيانات قريبة من الجهاز وتسريع الأداء. هناك عدد من الطرق لتنفيذ هذه التكنولوجيا والتحدي في تطبيقها والوصول إليها بشكل مناسب. ولكن تبقى الأمور خطرة للغاية من خلال اختراق نطاقات الأمن السيبراني لتلك البيانات وخوادمها لتجعل الأمور أكثر صعوبة على أنظمة الذكاء الاصطناعي. نشهد اليوم الكثير من النمو مع كل من أنظمة الذكاء الاصطناعي وإنترنت الأشياء. تتحد هذه التقنيات لتمكين المستوى التالي من الأتمتة والإنتاجية مع تقليل التكاليف. مع بدء

المستهلكين والشركات والحكومات في السيطرة على إنترنت الأشياء في مجموعة متنوعة من البيئات، سيتغير عالمنا إلى حد كبير ويسمح لنا جميعًا باتخاذ خيارات أفضل. إنه بالفعل يغير كل شيء بسرعة من التجزئة إلى سلسلة التوريد إلى الرعاية الصحية. تعمل IoT المدعومة من أنظمة الذكاء الاصطناعي على تحويل صناعة الطاقة من خلال حلول الطاقة الذكية، حيث تريد مدينة ذكية (smart city) أو إنشاء مدينة لتجارة الطاقة الكهربائية تنتج كميات كبيرة من الطاقة المحلية بسبب المنازل التي تحتوي على ألواح شمسية وتريد توريد تلك الطاقة خارجها بكفاءة كبيرة. يشارك الكثير من الخبراء تلك الرؤية المفرطة في التفاؤل ويعطون مثالاً على كيفية تغيير إنترنت الأشياء في سلسلة التوريد والخدمات اللوجستية. في هذا المثال، يكون اللبن عرضة للتغيرات في درجة الحرارة ولذلك ينبغي استخدام الذكاء الاصطناعي لتتبع تلك التغيرات، ويبقى أمن البيانات هو الهاجس الكبير لتلك التقنيات مع تزايد التهديدات السيبرانية. هناك سبب للتفاؤل من أن الذكاء الاصطناعي في الإنترنت سوف ينمو، بالنظر إلى الحالة الراهنة لنضج الذكاء الاصطناعي، فإن المنتجات المصممة بعناية لحالة استخدام محددة تميل إلى أن تكون أكثر فعالية من تلك المنتجات ذات النهج العام. في عام 2020، سنرى أول علامات التبني الملموس للذكاء الاصطناعي داخل المؤسسات الصناعية حول حالات استخدام رأسية محددة في إشارة بشكل خاص إلى مشهد IoT. ولذلك سيستمر استخدام الذكاء الاصطناعي في النمو والنضج، وكلما كان الاستخدام أكثر استهدافًا وتحديداً، كلما أصبح أكثر دقة. أذ أن توسيع النطاق يضيف التعقيد ويقلل من الكفاءة. تشمل الأمثلة الحديثة والحية لانتهاكات البيانات، التي بدأت عبر أجهزة إنترنت الأشياء المعرضة للخطر، ما يلي:

- تسرب بيانات الكازينو Crown - casino عام2011. عبر مقياس حرارة ذكي مرتبط بـ«الواي فاي»؛ حيث تمكن المتسللون من الوصول إلى شبكة الشركة، واسترجعوا البيانات المتعلقة بالعملاء ذوي الأجور المرتفعة، ثم استخرجوا البيانات مرة أخرى من خلال جهاز استشعار درجة الحرارة وفي السحابة.

- تم اختراق شركة Equifax للائتمان المصرفي والتجاري للحصول على معلومات ائتمانية لحوالي 143 مليون مستهلك. كان هذا الاختراق ناجحًا بسبب مشكلة عدم حصانة Apache Struts التي كانت منذ أشهر مسألة عرفتها Equifax ولكنها فشلت في حلها.

- جندت ميراي البرمجيات الخبيثة أجهزة Linux IoT الضعيفة في شبكات روبوت لتوصيل هجمات DDoS الرئيسية التي تحطمت عدة مواقع ويب. بحثت البرامج الضارة عن أجهزة إنترنت الأشياء التي لا تزال تستخدم أسماء المستخدمين وكلمات المرور الافتراضية للمصنع.

- سبر جميع أنحاء المدينة في مدينة دالاس بولاية تكساس على جميع صفارات الإنذار الطارئة البالغ عددها 156 صوتًا. أرسل هذا الاختراق تعليمات وهمية من خلال نظام التحكم اللاسلكي لصفارات الإنذار.

- اختراق منظومة Orvibo وهي شركة صينية تدير منصة IoT لإدارة الأجهزة المنزلية الذكية. تركت الشركة قاعدة بيانات تحتوي على معلومات مفصلة لأكثر من مليون عميل يتعرضون للإنترنت دون أي كلمة مرور لحمايتها. تطلب هذا الاختراق فقط كتابة عنوان URL بسيط في سطر عنوان المتصفح.

في حديث له في DEFCON في لاس فيجاس، ألقى برايسون بورت، الرئيس التنفيذي لشركة Scythe، ورئيس مجلس إدارة GRIMM ومستشار معهد Cyber Institute في ويست بوينت الضوءَ على بعض الاتجاهات الأكثر مغزى في مجال الأمن السيبراني إنترنت الأشياء وأنظمة التحكم الصناعية في العام 2018.

من وجهة نظر المستهلك، فإن أكبر المخاوف الأمنية بشأن إنترنت الأشياء تتعلق بالخصوصية. قد تشعر الأسرة بالقلق من أن كاميراتها الأمنية قد تعطي شخصًا غريبًا لمحة عن منزله. أو أن البيانات التي يجمعها مكبرات الصوت الذكية ضعيفة. مهاجمة أجهزة إنترنت الأشياء كنقطة محورية في حروب المستقبل هو أمر حقيقي. أن خطر قيام مهاجم بالتجسس عليك أثناء خروجك من الحمام عبر كاميرا متصلة بالإنترنت أمر حقيقي. لكن هذا النوع من الانتهاك لا يتماشى مع الأهداف الأكثر شيوعًا للجهات الفاعلة في التهديد المتمثلة في تحقيق مكاسب مالية أو التجسس المستهدف من جانب الشركات أو الحكومة. ومع ذلك، هناك تهديد أكثر أهمية وهو استخدام أجهزة إنترنت الأشياء للهجمات الجانبية. يعتبر اختراق العديد من أجهزة إنترنت الأشياء سلعة نسبيًا، ويوفر نقطة انطلاق لمزيد من التجسس أو التخريب. أفاد مركز الاستجابة الأمنية من Microsoft أنه لاحظ وجود عنصر تهديد يستهدف «هاتف VOIP وطابعة مكتب وفك تشفير الفيديو». وكان

الدافع الواضح للمهاجم هو الوصول إلى مجموعة متنوعة من شبكات الشركات. «بمجرد أن يكون الفاعل قد نجح في الوصول إلى الشبكة، فإن مسح الشبكة البسيط للبحث عن الأجهزة الأخرى غير الآمنة سمح لهم باكتشاف الشبكة ونقلها بحثًا عن حسابات ذات امتيازات أعلى تمنح حق الوصول إلى البيانات ذات القيمة الأعلى»، وأوضح التقرير، أرجعت Microsoft النشاط إلى مجموعة تسميها «Strontium»، والتي تعرف أيضًا باسم of Fancy Bear APT 28. ويعتقد أيضًا أن الجماعية قد شاركت في اختراق DNC في عام 2016. من ناحية أخرى قد لا تقل أهمية عما قدمناه آنفًا، فتمامًا مثلما تصمم شركات صناعة السيارات تصاميم لتضمن جودة وسلامة منتجها على المستهلك في الطريق، تحتاج المنظمات والشركات المصنعة لإنترنت الأشياء أن تسعى إلى تخفيف ثغرات الأمن السيبراني على الأجهزة المنزلية أو في الشركات المزودة بالإنترنت. سوف تندهش من عدد المنظمات والجهات التي تخطت هذه الخطوة تمامًا، وعدد المنظمات التي لا تعرف حتى ما هو نموذج التهديد، ناهيك عن تطبيقه. هذا هو المستند التأسيسي الذي يساعدك على فهم مكان بتخصيص مواردك. في جوهر اختبارات السلامة للإنترنت الأشياء الذي يجب تطبيقه وتعميمه بالسرعة الممكنة، هناك مبدأ ينطوي على البحث عن أخطاء في تكنولوجيا المعلومات - بمعنى آخر، الثغرات الأمنية ومعالجتها. في نهاية الأمر فالأمن حلقة لا تنتهي أبدًا. بالنسبة للعديد من الأفراد، هذا أمر مُحبط، لأنه لا يوجد خط نهائي محدد بوضوح.

3.2 إنترنت الفقاعة الهوائية

هل سبق لأحد أن رأى فجوة إنترنت هوائية حقيقية؟لا، لأنها غير موجودة بالفعل. من الناحية النظرية المجردة، فإن الشبكة ذات الهواء معزولة ماديًّا عن بقية العالم، مما يجعلها محصنة ضد الهجمات التي تجتاز الإنترنت. في الواقع، تواجهُ العديدُ من المنظمات التي تستفيد من مقاربة الأمن السيبراني عن طريق الغموض خطرًا كبيرًا من الانتهاك. هنا يتجلى المثال الأكثر شهرة لخرق نظام مزعوم محاط بالفقاعة الهوائية بواسطة الفيروس الشهير Stuxnet. في هذا الخرق، تمكن المهاجم من الوصول إلى شبكة داخل منشأة نووية إيرانية - ربما عبر مفتاح USB. على الطرف الآخر من العالم أصبحت شبكة الكهرباء الأمريكية عرضة للهجوم السيبراني، وقد اكتسبت سمعة سيئة بفضل جهود الصحفيين المخضرمين مثل تيد كوبل، الذي يغطي كتابه «إطفاء الأنوار» لعام 2015 هذا الموضوع. إذْ تمكن وفي العام ذاته (2015)، متسللون روسيون مزعومون من

التسلسل وتمهيد الإغلاق المؤقت لحوالي 230000 شخص في أمريكا. في غضون ذلك، نشرت الصحف الأمريكية سلسلة من المقالات التي تزعم أن روسيا تستهدف شبكة الطاقة الأمريكية. في الآونة الأخيرة، تكشّف النقاب عن أن الولايات المتحدة تستهدف روسيا أيضًا. يطرح هذا الوضع سؤالًا عن السبب وراء استخدام البلدان في جميع أنحاء العالم لتكنولوجيا المعلومات بشكل كبير في شبكات الطاقة الخاصة بهم إذا كانت تقدم مجموعة من التهديدات الجديدة. سأل أحد خبراء أمن البنى التحتية للطاقة: «لماذا لا نعود إلى سيطرة الشبكة التماثلية (Analog) تمامًا؟جزء من الإجابة على السؤال هو الطاقة الخضراء. هناك مجموعة من العوامل، مجموع كبير من الناس في جميع أنحاء العالم يتجهون إلى الطاقة الخضراء منهم من يشترون السيارات الكهربائية إلى تركيب الألواح الشمسية على أسقفهم، وهذه السلوكيات الاستهلاكية غيرت بشكل أساسي من معادلة توزيع الطاقة. قبل بضعة عقود، كان تدفق الإلكترونات من محطة فرعية إلى المستهلك أحادي الاتجاه. لكن الآن، أصبح المستهلكون هم المصدرون للكهرباء، من خلال مصادر الطاقة المتجددة مثل الطاقة الشمسية، يساهمون بشكل متقطع في إعادة الطاقة إلى الشبكة.

في عام 2017، ذكرت صحيفة نيويورك تايمز أن إدارة ترامب طلبت أربعة مليارات دولار للمساعدة في تمويل الأسلحة السيبرانية؛ لتخريب أنظمة مراقبة الصواريخ في كوريا الشمالية. إضافة إلى دعم تطوير الطائرات بدون طيار والطائرات المقاتلة لإخراج هذه الصواريخ من السماء قبل وصولها إلى الشواطئ الأمريكية. نقلت الصحيفة ذاتها عن مصادر مجهولة أن حملة إلكترونية جارية قد استهدفت أنظمة الصواريخ في البلاد منذ عام 2014 على الأقل. لم يظهر حتى الآن ما إذا كانت الولايات المتحدة قد عملت بشكل مكشوف على تطوير الهجوم السيبراني. لكن ما هو مؤكد هو أن الهجوم السيبراني الفردي يمكن أن يتسبب بمئات الملايين من الدولارات من الضرر. بعبارة أخرى، فإن Cry Wanna ومشتقاته لا تركز صراحةً على IoT أو ICS. لكن البرامج الضارة، التي تستهدف أنظمة تشغيل Microsoft Windows، ألحقت أضرارًا مماثلة بضحاياها. أظهر Wanna Cry أن قطعة من البرامج الضارة يمكن أن تعرقل عمليات الخدمة الصحية الوطنية (NHS) في المملكة المتحدة. بلغت تكلفة البرامج الضارة لـ NHS، والتي أدت أيضًا إلى إلغاء 19000 موعد، بمبلغ إجمالي 92 مليون جنيه إسترليني. وفي الوقت نفسه، كلف Wanna Cry not Petya، مجموعة شركات الشحن العالمية ما بين 200 إلى 300 مليون دولار. بعد إدخال البرنامج الضار إلى مصنع التصنيع عبر مورد حساس، كانت الصورة الذهبية للمصنع قديمة جدًا

ولا يمكن تصحيحها. بعد نشر متغير Wanna Cry في البيئة، «أضر بكل شيء يمكنه لمسه وأزال المصنع بالكامل».

أن حملات البنية التحتية الحرجة لإنترنت الأشياء تتصاعد، قد تكون هناك أمثلة قليلة نسبيًا للإشارة إلى المكان الذي تأثرت فيه قطاعات واسعة من السكان في جميع أنحاء العالم بالهجمات الإلكترونية القائمة على البنية التحتية الحرجة. لكنّ عددًا متزايدًا من المتسللين يستهدفون هذه البنية التحتية. النقطة الأساسية هنا مع هجمات البنية التحتية الحرجة هي أن هذه حملات استخبارات متكررة.

في عالم متصل، الموردون جزء من نموذج المخاطر، نعم إنه أحد التحديات التي تواجه المستهلك، أن الموردين هم المشكلة في حدوث الاختراقات الأرمنية لبياناتهم، في العام الماضي، أحدثت بلومبرج موجات من التظاهرات من خلال اتهام الصين بالتسلل إلى سلسلة الإمداد الأمريكية (Hardware US markets suppliers) من خلال تسوية أحد أكبر موردي اللوحات الأم (Motherboards) للخوادم في العالم. وقد عارضت القصة العديد من قادة شركات التكنولوجيا ذات الأسماء الكبيرة المذكورة في القصة، بما في ذلك SuperMicro وApple وAmazon بالإضافة إلى ممثلين من وزارة الأمن الداخلي الأمريكية والمركز الوطني للأمن السيبراني بالمملكة المتحدة. على الرغم من أن حقائق المقالة ذات الصلة قد تكون محل تساؤل، فإن ما يسمى «العيش خارج الأرض» يمثل تهديدًا. «المهاجمون لا يجلبون أدواتهم إلى اللعبة. إنهم يأخذون ما هو موجود بالفعل في تلك البيئة ويستخدمونه ضدك. «أي شيء يمس البنية التحتية الخاصة بك هو جزء من نموذج المخاطر الخاص بك كمستهلك. لم تعد أنت فقط بعد الآن في ساحة تلك الحرب الرقمية، إننا نعيش أحداثا مشابهة لفيلم ماتريكس». البيانات الخاصة بك تتكاثر وتنمو. هكذا يتم بيعها. «هل تعلم أن التلفزيون الذكي يتكلف أقل من التلفزيون العادي بدون أي وظيفة ذكية؟» «لماذا هذا؟إنهم يكسبون المال من القياس (remote measurement) عن بُعد وبياناتك هي السلعة التي يروجون لها باستمرار. تصل مقالة Business Insider عام 2018 إلى نفس الاستنتاج حيث «تقوم بعض الشركات المصنعة بجمع بيانات حول المستخدمين وتبيع هذه البيانات إلى جهات خارجية. يمكن أن تتضمن البيانات أنواعًا، وعدد العروض التي تشاهدها، والإعلانات التي تشاهدها، والموقع

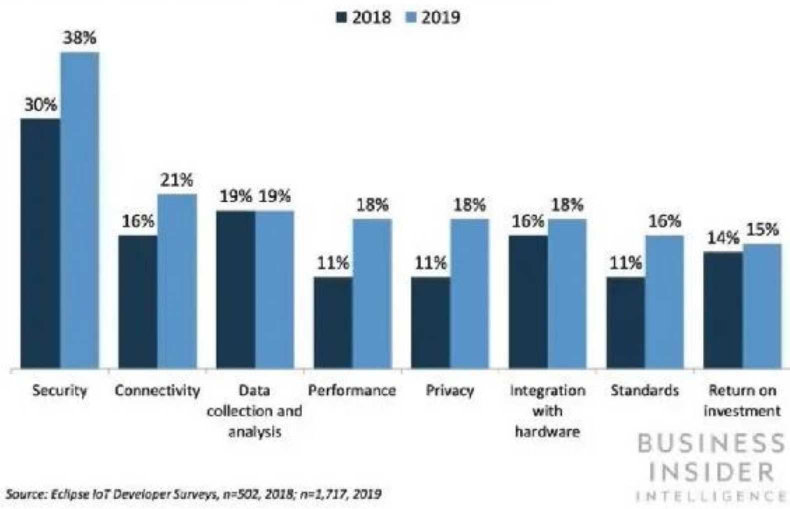
الجغرافي التقريبي. «إن بعض شركات صناعة السيارات تنشر أساليبَ مماثلةً بالفعل. إذْ أن هناك نماذج متعددة يبحث فيها صانعو السيارات عن كيفية وما يمكن أن يأخذوه منك عندما تقود سيارتك.!

في عصر الذكاء الاصطناعي الذي يهيمن على مقدرات معظم التكنولوجيا التي تنتج اليوم من خلال تقنية التعرف على الوجوه أو السيطرة الذاتية على الأجهزة والمتحسسات ومن خلال المسح الذكي للكثير من الفعاليات والأنشطة البارومتري للمستخدم ودمجها مع استعمال الأجهزة المنزلية! بالطبع ستقوم تلك التقنيات بدعم عمل تلك الأجهزة وتكاملها ودقة عملها في نهاية المطاف. ولكن مع ازدياد وتيرة التقدم التقني المضاد والذي يقصد به التقدم التقني الذي له غايات إجرامية وخطيرة مثل جمع البيانات الشخصية وتعقب الأهداف والمراد منها سرقة المحفظة المالية لشخص أو شركة معينة. لذلك لا يمكن فصل تلك التقنيات المتطورة عن غايات التجسس الأخرى التي يسيل لها لعاب الأطراف الإجرامية وحتى الأطراف الحكومية لأن الحكومات في طبيعة تكوينها تفضل التجسس على مواطنيها بأي شكل من الأشكال. ولذلك كانت هناك أحد الأمثلة الصارخة على اختراق الأجهزة الذكية في المنزل من خلال ربطها مع إنترنت الأشياء والمثال هنا كانت الثلاجات الذكية والتي تمتلك العديد من التقنيات والأنظمة التكنولوجيا المتكاملة معه مثل: الكاميرا ومتحسسات درجة حرارة ومتحسسات فتح وإغلاق الباب وكذلك متحسسات لمسية وفي إحدى الحالات كان المستخدم يقوم به إدخال بيانات الأطعمة التي جلبها إلى المنزل وبعد ذلك كانت هناك كاميرا لمسح الوجه والتعرف عليه وفي إحدى الحالات كان المستخدم يقوم به إدخال بيانات الأطعمة التي جلبها إلى المنزل وبعد ذلك كانت هناك كاميرات حرارية للتعرف على الوجه وإعطاء النصائح الإرشادية للوجبات الغذائية، وخلال الحوار بين المستخدم و الثلاجة الذكية تم تسجيل ذلك الحوار ونبرة الصوت واستخدامها من قبل الشركة الثالثة والمشتركة في تصنيع بعض أجزاء الثلاجة واخترقت الحساب المصرفي لهذا الشخص عن طريق الخطأ. ومنها برزت مشاكل الطرف الثالث الذي ساهم في دعم أو تصنيع بعض أجزاء تلك الأجهزة المنزلية الذكية.



الشكل (2) صورة فوتوغرافية لشكل الثورة القادمة في إنترنت الأشياء عندما تطلب الثلاجة الخاصة بكمية الحليب التي أريدها - ماذا تعني ثورة IOT تسويق العلامات التجارية؟(المصدر: Sawhney Jasmeet)

ولم يقتصر الأمر على ذلك بل وتعداه إلى أن تكون تلك الثلاجة وأجهزة الاستشعار التابعة لها أو المدمجة فيها قامت بجمع البيانات وتبويبها من خلال فيروس اختباري تم تجربته على ذلك الجهاز المنزلي وبشكل صادم، قام الفيروس بجمع كل المعلومات والبيانات التي حصل عليها بل وتعداه وذلك إلى جمع البيانات الشخصية من أجهزة أخرى مرتبطة بتلك الثلاجة من خلال شبكة إنترنت الأشياء المنزلية. يشير الشكل (3) إلى المشاكل الكبيرة المرتبطة بإنترنت الأشياء وعلى رأسها الأمن السيبراني واختراق الخصوصية للمستخدم.



الشكل (3) زيادة الحلول التقنية لإنترنت الأشياء وتطبيقاتها المتعددة خلال عامين فقط (2018 - 2019) وزيادة المشاكل المتعلقة بتلك الحلول والتطبيقات وأهمها هي الأمن السيبراني ومتفوقة بنسبة 38% خلال العام المنصرم فقط (المصدر: ايكلبس للمسح التطويري لإنترنت الأشياء).

وبالتأكيد ربما يتم تعميم تلك الحالة المفردة على أجهزة ذكية أخرى موجودة في المنازل فمثلا في التلفزيون الذكي وخاصة من النماذج الحديثة التي أنتجتها شركة مشهورة مثل: (الـجي وسامسونج وباناسونيك) والتي تحتوي على أجهزة غاية في التقدم التقني مثل الكاميرات الذكية والتي تستشعر حركة الإنسان من على مسافات بعيدة وكذلك ميكروفونات مدمجة وموزعات صوتية إضافة إلى مستشعرات الذبذبات الميكانيكية وكذلك نظام توزيع الصوت كل تلك الأجزاء لها القابلية على خزن المعلومات وتتبع حركة الأشخاص الذين يشاهدون التلفاز الذكي ولهذا يعتبر التلفاز أداة تجسس مثالية إذا ما تمّ مقارنته بباقي الأجهزة المنزلية المدمجة في شبكة إنترنت الأشياء. طبعا إذا تابعنا الأخبار حول إنترنت الأشياء سوف نعلم بأن أحد الهموم التي تأتي إلى خبراء التقنية وهي اختراق الخصوصية وأصبح هذا الأمر مفروغًا منه وبالطبع فإنّ تلك القضايا أصبحت واقعًا حقيقيًّا وازدادت بشكل ملحوظ حتى أقنعت الكثير من الخبراء المختصين في اختبار تقنية إنترنت الأشياء أن تلك التقنية يسهل اختراقها من قبل أبسط أنواع الهاكرز (قراصنة شبكات الإنترنت). وأصبحت تلك المشكلة أكبر تهديدا لنجاح إنترنت الأشياء في غزو السوق الاستهلاكية، في حزيران عام 2019 كان هناك أشبه بسيل من قضايا الاختراق الخاصة بتقنية إنترنت الأشياء ونشرت حلقة جديدة من الأخبار متابعة الزيادة الغريبة في الاختراقات المتكررة مما ساعد على دقّ جرس الإنذار لمستخدمي تلك التقنية بأن يعطوا انتباههم بما قد يحدث للبيانات التي يتم جمعها بواسطة أجهزة إنترنت الأشياء.

في بعض الحالات كانت هناك شركات تقوم بتصنيع أجهزة منزلية بسيطة مرتبطة بالإنترنت ومنها شركة الجرس Ring والتي تمتلكها شركة أمازون؛ حيث عملت هذه الأخيرة بالتعاون مع أقسام الشرطة لبناء شبكة من المراقبة التلفزيونية لكل المناطق السكنية التي اشترت منتجاتها، وتعدى الأمر في بعض المناطق إلى قيام الشركة بالتعاون مع أقسام الشرطة في إحدى المدن الأمريكية لزيادة أجراس الباب الرقمية والمزودة بكاميرات دعم المراقبة المستمرة للشوارع والأزقة في تلك المدن. هذا التعاون الغريب من نوعه بين شركات تجارية وأقسام الشرطة المحلية يعتبر من وجهة

نظرنا نوعًا من اختراق الخصوصية في مناطق سكنية بعينها اعتمادًا على تقنية إنترنت الأشياء. لم يمضِ وقت طويل على اعتبار «IoT security» كجملة كاملة مشبعة بالتناقضات وكذلك هو الإدراك والوعي لأهمية الموضوع؛ فنظرًا للتوسع الكبير في عدد الأجهزة المتصلة داخل كل شيء تقريبًا بدءًا من المباني وحتى المصانع، لم يكن لدى الخصوم أبدًا مجموعة متنوعة من نقاط النهاية المتاحة لهم لاستهدافها. هنا، نعرض ما الذي سيحدث في لعبة القط والفأر التي تمثل الأمن السيبراني الأعوام المقبلة إذْ تنمو المخاوف الأمنية في الأبنية بشكل سريع، بِدءًا من عام 2020، سيصبح أمن المباني الذكية أكثر أهمية بالنسبة لمديري المنشآت. مع وجود حوالي ثمانية من أصل عشرة أشياء متصلة في المباني في عام 2020! فوفقًا لما ذكره غارتنر، يمكن للمباني الذكية أن توفر طرقًا جديدة للخصوم للهجوم. ومع ذلك، فإنّ الخبراء منقسمون حول ما إذا سيكون هناك ارتفاع كبير في مثل هذه الهجمات العام المقبل أو الأعوام التي تليها. يتوقع Mirel Sehic، المدير العالمي للأمن السيبراني لشركة Honeywell Building Solutions حدوث مثل هذه الزيادة. إذْ يمكن للمهاجمين - حسب هذه الاحتمالية - استخدام أنظمة إدارة المباني كنقطة محورية للوصول إلى بيانات تكنولوجيا المعلومات وكذلك لمعالجة ضوابط المبنى.

يقول أحد خبراء الأمن السيبراني لإنترنت الأشياء أندرو هاوارد، الرئيس التنفيذي لشركة بودولسكي سيكيوريتي: «لا أعرف أننا سنرى المزيد من التهديدات هناك العام المقبل». لدعم هذا البيان، قال هوارد إن الشبكات داخل العديد من المباني مجزأة للغاية. وأوضح «رغم أنه قد يكون هناك نظام واحد متصل بالإنترنت، فإن الواقع هو أن معظمهم ليسوا كذلك». «وإذا كان الأمر كذلك، فإنها تميل إلى أن تكونَ WLAN مثبتةً على الشبكات المعزولة. لا يشبه الكثير من شبكات إنترنت الأشياء التي تراها هناك حيث توجد جميع هذه الأجهزة في بعضها مثل هندسة الشبكات المسطحة (Flattened network engineering). أصبح احتمال بناء أنظمة شبكية للمؤسسات والأبنية مصدر قلق بارز للأمن السيبراني بعد خرق بطاقة الائتمان المستهدفة لعام 2013. في تلك الحادثة، تم انتهاك البيانات لأحد بائعي أنظمة التكييف HVAC في إحدى متاجر Target، مما سمح للمهاجم بالوصول إلى شبكته الداخلية، بما في ذلك نظام الدفع الخاص به (payment system). في تلك الحلقة، قام المتسللون بسرقة معلومات أربعين مليون بطاقة ائتمان. فللنظر لحجم ثغرة أمنية واحدة لنظام لم يكن يخطر على بال!

ما ذكرناه آنفًا مرتبط بتقنية الإنترنت «G4». لكن وفي النصف الأول من العام 2019، كانت هناك عروض تجريبية في المعارض التجارية والمواقع الفردية على المستوى الجديد «G5» إذ بدأت شركات الاتصالات في بناء شبكات الجيل الخامس الخاصة بها بحيث يصبح «G5» بروتوكولًا أساسيًّا في نهاية المطاف مما قد يعني أن كل شيء بدءًا من كاميرات المراقبة وحركة المرور وحتى المركبات مرتبط عبر البروتوكول. هذا التغير الذي يبدو تطورا طبيعيًّا سوف يمنح المهاجمين وسائل بسيطة لشلّ الأحياء أو المدن أو حتى بلدان بأكملها. الـ «G5»، مثل غيرها من الشبكات اللاسلكية wireless network، عرضة لهجمات الحرمان من التشويش والتشويش المضاد. بدأت خلال الفترة السابقة شركات الاتصالات والبنية التحتية تروج لـ «G5» لمجموعة من حالات الاستخدام المحدود، بما في ذلك المجال الصناعي والطبي. تعتبر إمكانية استخدام «G5» في العمليات الصناعية الحرجة ذات التأثير الملموس على الأعمال اقتراحًا ينطوي على مخاطرة كبيرة. كما نبّه إليها العديد من الخبراء والمختصين الذين هم على تماس كبير مع تلك المخاطر ومنهم جيسون هاوارد غراو، كبير مسؤولي أمن المعلومات في شركة PAS Global، إن الأمور المعقدة في هذه النقطة بالذات هي حقيقة أن العديد من البيئات الصناعية تنشر «أجهزة قديمة وغير مواكبة التحديثات التقنية الجديدة». وأضاف نقطة هامة في تصريحاته: «سيبدأ الخصوم باستهداف هذه البيئات، مما يؤدي إلى عواقب وخيمة مثل التغييرات غير المصرح بها على التكوينات التي تجعل العمليات الصناعية تفعل شيئًا ليس من المفترض أن تفعله، مما ينتج عنه حادث صناعي أو انقطاع أو حتى رحلة بيئية».

بالطبع لم تتوقف الحكومات من التدخل في أنظمة التشغيل والبرمجيات التي تعمل عليها أجهزة إنترنت الأشياء فعلى سبيل المثال بعد أشهر من حظر روسيا بيع الأدوات التي لم يتم تثبيتها مسبقًا مع البرامج الروسية الصنع، قام المسؤولون الحكوميون في ذلك البلد بصياغة إرشادات جديدة بشأن أنواع شركات البرمجيات التي قد تحتاج إلى تثبيتها. حيث تم إنشاء تلك الإرشادات، التي تنطبق على الهواتف الذكية وأجهزة الكمبيوتر وأجهزة التلفزيون الذكية، بواسطة الخدمة الفيدرالية الروسية لمكافحة الاحتكار، ويذكرون في تلك الإرشادات أن هذه البرامج يجب أن تراعي في طبيعتها «تشكيل أولوية القيم الروحية والأخلاقية الروسية التقليدية» ويجب أن يكون عموميًّا وآمنًا للمستخدم. لكن دعونا نحلل تلك الجملة الموجودة في الإرشادات عن ماهية تلك القيم الروحية والأخلاقية التي تشدد الجمعية الروسية على اتباعها؟فهل هي تضم من خلال ذلك قدرة التسلل

لوكالات الأمن الروسي على تلك البرمجيات والأجهزة التي تم تنصيبها عليها؟! ومع ذلك، لم تحدد مسودة المبادئ التوجيهية القيم الروسية التي يجب أن يتماشى البرنامج معها. أقرت البلاد قانونًا يحظر بيع الأدوات بدون برامج روسية مثبتة مسبقًا في نوفمبر الماضي. قال المؤيدون إن هذا القانون يهدف إلى تعزيز التكنولوجيا الروسية وجعله من السهل على الناس في البلاد استخدام الأدوات التي يشترونها. لا يعني القانون الروسي المثير للجدل، الذي سيدخل حيز التنفيذ في يوليو 2020، أن المنتجات التي تحتوي على برامج مصنوعة في بلدان أخرى لا يمكن بيعها في روسيا، ولكنها تتطلب منهم أيضًا تثبيت خيارات برامج روسية بديلة. في الواقع العملي لم يتم تبني القانون من قِبل الشركات المصنعة والموزعين المعتمدين لتلك الأجهزة في روسيا. قالت رابطة الشركات التجارية والشركات المصنعة للمعدات الكهربائية المنزلية وأجهزة الكمبيوتر (RATEK) أنه لن يكون من الممكن تثبيت البرامج الروسية الصنع على بعض الأجهزة. كما ذكرت أن الشركات الدولية، مثل Apple، التي تصنع تلك الأدوات والأجهزة قد تنسحب من السوق الروسية بسبب هذا القانون الغريب.



الشكل رقم (4) مخطط عام يوضح التهديدات المتعددة لأمن البيانات في وسائط إنترنت الأشياء والمخاطر الكبرى التي تعمل على تحطيم تلك الشبكات التي زادت أهميتها بالنسبة للمستخدمين خلال السنوات الأخيرة.

الفصل الرابع

غياهب رقمية الملاذ الآمن

4.1 الإنترنت المظلم

«هذه الحرب السيبرانية ستستمر مثل حرب
ماراثونية
وستكبر وتتطور في التخفي بطرق معقدة وتسهل
الدخول
لطالبي خدماتها نظرا للتطور السريع في هجماتها
الاستراتيجية لبيع تلك الخدمات على الويب
المظلم»

جيمس سكوت - خبير الأمن المعلوماتي في
معهد البنى التحتية الحرجة

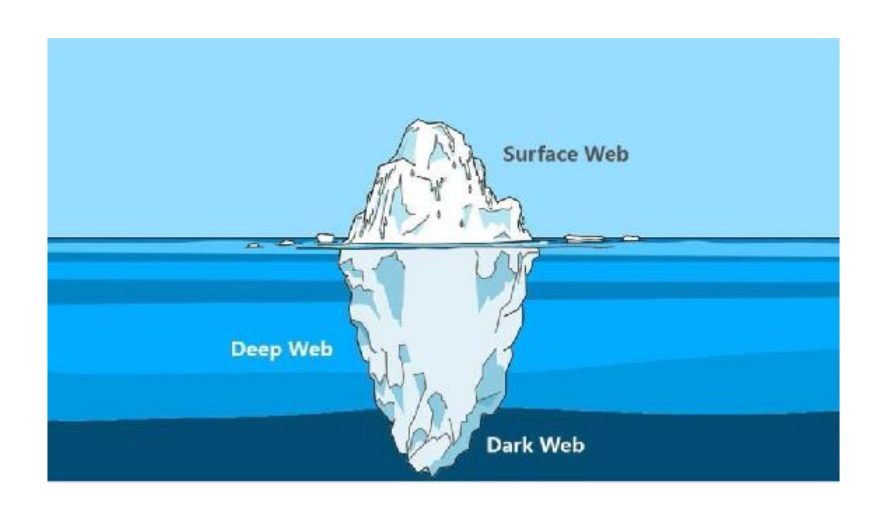
كانت البداية في إحدى الاختبارات التي كانت تعمل على مشروع الإنترنت الخفي (Invisible Internet project) والذي يعرف اختصارًا ب- «مجال البصلة Onion domain» حيث كان الهدف من هذا المشروع هو إخفاء هوية مستخدمي الخدمات المرتبطة به كما يتم إخفاء هوية وأماكن المواقع الإلكترونية التي تم إنشاؤها فيه. تم مرور البيانات في النقاط الأساسية؛ لتدفق المعلومات في الويب المظلم من خلال العديد من الخوادم الوسطية التي تحمي هوية المستخدم، وتعمل على توثيق إخفاء هويته، مرّ هذا المشروع بالعديد من المحطات التطويرية التي ساهمت في خروجه بهذا الشكل المحترف، والدقيق من محتويات مخفية عن عيون الحكومات والمؤسسات

الرقابية الأخرى؛ لذلك زادت شعبية هذا الموقع والمجالات المرتبطة به ونقصد بها مجالات الإنترنت واعتمدها المستخدمون له في تزويده والخدمات المرتبطة به وعلى رأسها المحتويات الإباحية للأطفال والعبودية الجنسية والأنشطة الإجرامية الأخرى، وكذلك تجارة الأسلحة والشبكات والاستغلال البشري، وشبكات الجريمة المنظمة، والابتزاز الإلكتروني، والسرقة الإلكترونية وغيرها من الأنشطة المناهضة للقوانين. انتشرت سُمعة الويب المظلم والمواقع المرتبطة به والخوادم الوسطية النهائية، التي تقوم بتخزين البيانات والمنتجات التي تعرض في مواقعها المختلفة وأصبح ملاذًا آمنًا لكل ما تم ذكره من أنشطة إجرامية أو مخالفة للقانون، ومن الجدير بالذكر أن هناك أيضًا نوعًا من أنواع الإنترنت شبه مخفي قد تم تطويره من قبل شركات صغيرة في آسيا وتحديدًا في «صنفرة» بهدف تنظيم عمليات البيع والشراء غير القانونية لبعض تجار المخدرات في تلك المنطقة. إنّ البوابة الرئيسية للكثير من المستخدمين العاديين للشبكة العالمية (Normal NIU Internet users) للدخول إلى عالم الإنترنت هو موقع محرك البحث الشهير Google والذي تحوّل فيما بعد إلى عملاق التكنولوجيا الرقمية والذكاء الاصطناعي؛ لما يقدّمه من خدمات في البحث وأرشفة المواقع وغيرها، في الحقيقة ما يُظهره الـ «جوجل» - أو حتى بقية محركات البحث - من مواقع شبكية هو جزء يسير جدًّا من المواقع والمعلومات الموجودة فعليّاً على الإنترنت، إذْ تشير بعض الإحصائيات إلى أنّ هذه النسبة حوالي 5% فقط من المعلومات والمواقع الفعلية الموجودة على الإنترنت. في الجزء العميق المتبقي من الإنترنت الذي لا تستطيع محركات البحث العادية أرشفته وعرضه لنا، يُطلق عليه مصطلح الإنترنت العميق أو Deep Web. من الناحية النظرية لوصول محرك البحث إلى المعلومات الموجودة على الإنترنت، يمكن تقسيم الإنترنت إلى:

أولاً: طبقة الإنترنت العادية Normal browsed Web تسمى في بعض الأحيان السطحية (web Surface) والتي تظهر ضمن محركات البحث جوجل وبنج (Bing) وثندربيرد (Thunderbird) وغيرها، والتي نستطيع الولوج إليها عن طريق متصفحات الإنترنت المعروفة، مثل موقع Wikipedia أو بريتانيكا، وغيرهما من المواقع. وتشكل ما نسبته 5% فقط من الإنترنت وهي نسبة ضئيلة جدّاً من الاستخدام الكلي للإنترنت بشكل عام.

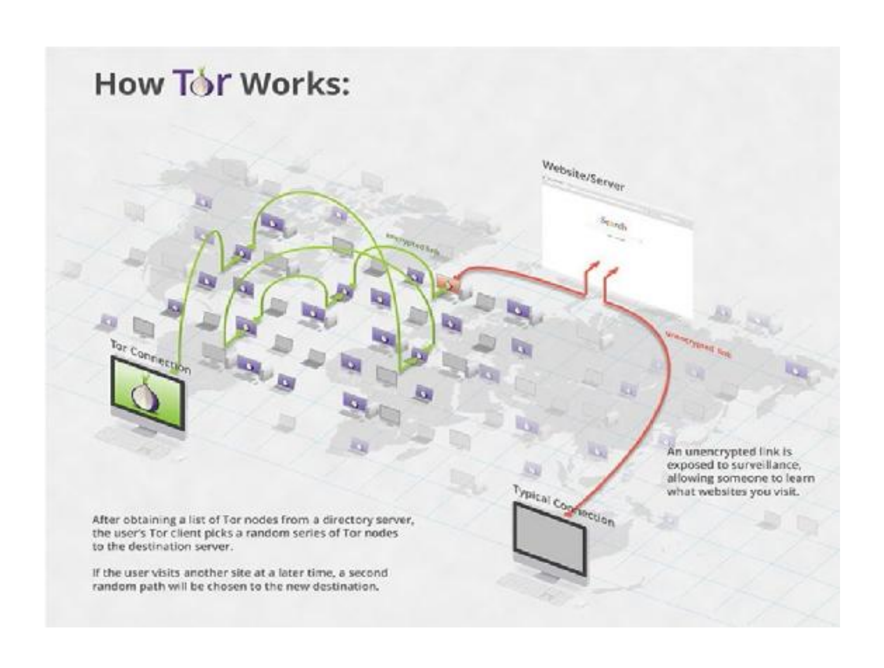
ثانياً: طبقة الإنترنت العميقة Deep Web: هذه الطبقة محجوبة عن محركات البحث، ولا تستطيع محركات البحث المعروفة أرشفتها وعرضها علينا، وتتخذ عدة أشكال، فأي معلومة أو

موقع أو صفحة إنترنت لا تستطيع محركات البحث أرشفتها تعتبر جزءًا من الإنترنت العميق. فمثلاً المعلومات البنكية لشخصٍ ما تعتبر جزءًا من الإنترنت العميق، ورسائل البريد الإلكتروني أيضًا تعتبر جزءًا من الإنترنت العميق، كما أنّ الكود البرمجي (programming code) الذي يُوَلّد صفحات ديناميكية (Dynamic page generators) لأي موقع يعتبر جزءًا من الإنترنت العميق، وأيضاً المعلومات السريّة لأي جهة أو حكومة لا يمكن الولوج إليها إلا عن طريق كلمات سر معيّنة تعتبر أيضًا جزءًا من الإنترنت العميق. كل هذه المعلومات لا يمكن لمحركات البحث الوصول إليها لأنها محمية فهي جزءٌ مخفيٌّ من دهاليز الإنترنت العميق.



شكل (5) يوضح أشكال الويب أو محتوى الإنترنت ومنه الإنترنت السطحي والعميق والمظلم والأخير يعتبر جزءًا كبيرًا من الويب العميق (المصدر: Hacker Noon)

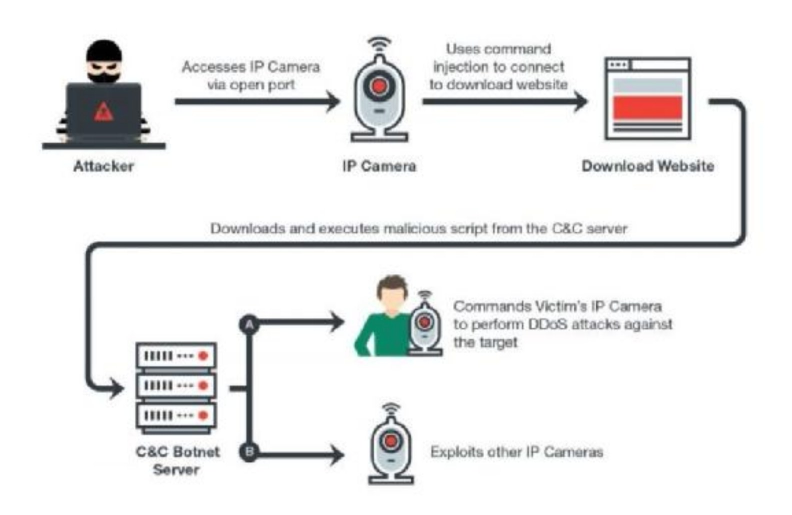
يعتبر عالم الإنترنت عالمًا كبيرًا جدًّا أكثر مما تتصور، كلنا يعلم عن مواقع التواصل الاجتماعي مثل: «الفيس بوك جوجل اليوتيوب أمازون» ومواقع الدردشة الرقمية مثل: «الواتس اب والماسنجر والتليجرام» كثيرًا، لكن هل تعلم ماذا يجري خلفه الواجهات؟هذا هو السؤال المهم بعضنا يعرف الإجابة عليه: ما سبق ذكره هو عبارة عن زاوية صغيرة في الإنترنت لكن الشبكة المظلمة والشبكة العميقة ما زالت تعمل في زوايا لم يصلها النور بعد، يتمكن المستخدم فيها من الوصول إلى هذه الزوايا من خلال استخدام برامج محجبة يستطيع من خلالها الولوج إلى الشبكة المظلمة والشبكة العميقة وأحد أشهر تلك البرامج برنامج تور المطور من قبل نخبة من المبرمجين الروسيين.



الشكل (6) مخطط انفوجرافيك لبرنامج الولوج للشبكة المظلمة (Tor) في عام 2004، تم إصدار Tor برنامج مفتوح المصدر. سمح هذا لـ Dark Web بالنمو لأن الأشخاص يمكنهم الوصول إلى مواقعهم بشكل مجهول.

لكن قبل الولوج إلى تلك الشبكات العميقة في الإنترنت ينبغي للمستخدم أن يعرفه طبيعتها ومحتوياتها وخطورة تلك المحتويات على سلامته سواء كان رقمية أو شخصية. إن مصطلح الشبكة المظلمة مطلق بشكل محدد على مجموعة من المواقع الإلكترونية تستخدم شبكات مشفرة ولا يمكن إيجادها في مواقع البحث العامة أو متى يتم زيارتها باستخدام متصفحات عامة (General browsers). بشكل عام كل المواقع الرقمية التي تدعى بالشبكة المظلمة (Dark web) تخفي حقيقتها. وهويتها الأصلية استخدام أدوات التشفير الخاصة ببرنامج تور هذا المتصفح يقوم بإخفاء هويتك وموقعك الجغرافي، وهو في هذا الأمر من الإدارات المتخصصة ذات القابليات الكبيرة في عمليات التشفير الرقمي ويقوم كذلك بإعطاء موقع جغرافي مختبر عن موقعك الحالي وهو في تقنية مشابه لتقنية الـ«في بي إن» (VPN). يشكل الـ «دارك ويب» جزءًا صغيرًا من الويب العميق وهو جزء من الويب لا تُفهرسه محركات البحث، ولكن أحياناً يُستخدم مصطلح «ديب ويب» بصورةٍ خاطئةٍ للإشارةِ إلى الـ «دارك ويب». أجرى الباحث غاريث أوين من جامعة بورتسموث دراسة في ديسمبر عام 2014، توصل فيها إلى النوع الأكثر شيوعًا من المحتوى على» تور» يتعلق بمواد

الاستغلال الإباحي للأطفال، ويليها الأسواق السوداء، في حين أن المواقع الفردية التي سجلت أعلى زيارة أو دخول كانت تلك المخصصة لعمليات البوتنت (botnet). وكذلك منتديات النقاش السياسي ومواقع التواصل الاجتماعي الأخرى. إذا حسب التعريف العام لشبكة الروبوتات الرقمية وهي عبارة عن شبكة من الروبوت (بالإنجليزية: Botnet) مجموعة ضخمة (يبلغ تعدادها بالآلاف وقد يصل للملايين) من الأجهزة التي تم اختراقها عن طريق الإنترنت كل واحد منها يسمى بوت تخدم مكون البوتنت أو ما يسمى بسيد البوت (Bot Master). يستخدم سيد البوت قناة أوامر وتحكم (C&and Control Channel C Command) لإدارة شبكته وتنفيذ هجماته، وتسمية البوتنت هذه مشتقة من كلمة (Robot Network) أي شبكات الروبوت حيث أن الأجهزة تخدم سيد البوت دون اختيارها، تمامًا مثل أجهزة الروبوت، وبمجرد أن ينضم الجهاز لشبكة الروبوت فإن البوت الماستر يستطيع التجسس على صاحب الجهاز دون أن يشعر بذلك.



الشكل (7) مخطط توضيحي يشرح كيفية اختراق الكاميرات المرتبطة ببروتوكولات الإنترنت والتي تستخدم على نطاق واسع في التطبيقات المنزلية والتجارية المختلفة، حيث يتمكن قراصنة الإنترنت من الولوج إلى خوادم تلك الكاميرات ومن ثم إلى خوادم الشركات المشغلة والاستيلاء على كل البيانات المسجلة لعملائها.

ولا يتوقف ضرر البوتنت على الأشخاص فقط، في البوتنت أحد أهم وأخطر المشاكل الأمنية التي تواجه الشركات والدول أحيانا وأبرز مثال لذلك الهجوم الذي وقع على دولة إستونيا عام 2007، حيث تعطلت مواقع الوزارات والشركات لثلاثة أسابيع! وتستخدم البوتنت في تعدين العملات الرقمية حيث تم استخدامها بشكل واسع في تعدي (Cryptocurrencies mining) العملة الرقمية بتكوين وليبرا والإيثريوم بشكل كبير وساهمت في دائرة أعمال الإجرام الرقمي والجرائم السيبرانية محتمل أنْ تقوم بعض المنظمات والفروع باستخدام الروبوتات الشبكية سيداره بعض صفحات وسائل التواصل الاجتماعي الفيس بوك وتويتر بعض الخدمات الملحقة بها. كما تقوم رابطات الشبكية عمليات السطو أرقامي على المحافظ المالية المخزونة الخوادم الخاصة العمليات المصرفية التي تستخدم خوارزميات التعدين الرقمي. وعلى الرغم من أنّ تلك الشبكات الروبوتية قد تم استخدامها في التأثير على الانتخابات السياسية والاستطلاعات الشعبية، أما الشبكة العنكبوتية رقم الخطوط في اختراق خدمات الشركات التجارية ومحافظ الأفراد الرقمية (Digital Wallets)

وضوء برامج التجسس ابتداء الهجمات المنسقة على النت وسرقة المعلومات الشخصية وكذلك استخدام الإعلانات المضللة والغرض منها خداع المستهلك.

4.2 ملاحقات حكومية

بعثت الكثير من المصادر الحكومية والمؤسسات غير الحكومية من مهام تتبع شبكات الويب العميق وشبكات الويب المظلم والتي ساهمت في كثير من الأحيان في كشف الجرائم والانتهاكات المستمرة لحقوق الإنسان في البلدان، تلك المؤسسات الحكومية؛ ولذلك كان من البديهي أن تقوم الحكومات والمؤسسات الأمنية الولوج إلى محتويات الويب العميق والمظلم معتبرة أنه كل من يقوم باستخدام تلك الأدوات هو مجرم بالضرورة وسخرت الكثير من عملائها وزودتهم بهويات رقمية مزيفة وعملت على استدراج الكثير من الناشطين السياسيين وجماعات حقوق الإنسان وألقت القبض عليهم من خلال استخدام شبكات الويب العميق والمظلم والتي بدورها الأساسي تعمل على توفير غطاء رقمي النشاطات تلك المؤسسات السياسية المناهضة للحكومة ومن خلال ذلك نرى أن الحكومات قد نجحت في الولوج بشكل سلس إلى تلك الشبكات محطمة بذلك آخر كلام الديمقراطية أو منابر التعبير السياسي والاجتماعي لمختلف النشطاء السياسيين. إذًا كيف يمكن لأولئك الناشطين أن يمارسوا انتقاداتهم واستئناف نشاطاتهم الاجتماعية والثقافية والسياسية المختلفة ضد هؤلاء الطغاة والديكتاتوريين الذين يسيطرون على كل مفاصل الحياة في البلدان المغلوب على أمرها. وهنا يظهر السؤال الملح لجميع حول مصطلح الإنترنت المظلم فهل جميع مستخدمي هذا الإنترنت هم من المجرمين والخارجين عن القانون؟

الجواب بالتأكيد كلا، فهناك اعتقاد شائع بين جمهور مستخدمي الإنترنت المظلم وهم من أرباب السوابق وقراصنة الحاسبات وتجارة البشر ومروج المخدرات وهذا بالأساس لا لبس فيه إلا أنه هناك نسبة كبيرة من مستخدمي الويب المظلم من الأشخاص الذين يحاولون منع الجرائم أو القيام بأنشطة سياسية مناهضة للحكومات الديكتاتورية. فمثلًا يستخدم الكثير من الناشطين الحقوقيين والموظفين في المنظمات الإنسانية الإنترنت المظلم في تبادل الأفكار والبرامج وتحشيد للتظاهرات أو إلى فعاليات اجتماعية وسياسية واقتصادية لدعم أعمالهم ضد الحكومات المستبدة إضافة إلى استخدام الكثير من العاملين في مجال أمن المعلومات وتشفير الرقمي الإنترنت المظلم يعتمدون على كان مصدر موثوق بمعلومات مهمة تتعلق بالثغرات الأمنية والاختراقات وتسريبات المعلومات

الحساسة. وبذلك تكون قيمة الإنترنت المظلم عالية جدًّا بالنسبة للخبراء في مجال أمن المعلومات والحماية المعلوماتية للمنشآت التي تحتاج إلى رؤية محترفة في مجال الحماية الرقمية، إضافة إلى ذلك فإن الكثير من هؤلاء الأشخاص المتدربين على استخدام الويب المظلم وخاصة من العاملين في مجال الأمن الحكومية والمؤسسات الرسمية رديفة الذين يعملون على ملاحقة المجرمين عن طريق تتبع برامج WeChat ويستخدمونها للإيقاع بتجار البشر، وتجار المخدرات وغيرهم من أصحاب النشاطات الإجرامية من خلال إخفاء هوياتهم الشخصية والفعلية على الإنترنت والعمل على ملاحقة هؤلاء المجرمين، وهناك نوع آخر من مستخدمي الويب المظلم وهم الصحفيون والذين يقومون في تحقيقات مفردة صحفية مع الكثير من الجهات التي لا تستطيع الإعلان عن هويته الحقيقية مثل جماعة أنونيموس المشهورة عالميا حيث تستخدم هذه الجماعات التقنية الإنترنت العميق كأول ملاذ لإخفاء فعالياتها وأنشطتها على الإنترنت، وبالتأكيد فإنّ كيفية إنشاء تلك المواقع المختلفة على الويب المظلم في الكثير من الحالات يتم بناؤها باستخدام نطاق أونيون Onion domain وهو نطاق الاستخدام العام لشبكات تور؛ حيث يمكن لأي شخص أن يحجز موقعًا باسمه المعين ولكن بطريقة مختلفة عن حجز الأسماء في النطاق العالمي، حيث يتولى أدوات برنامج التور عملية التسجيل هذه، وبالتالي فإنّ عملية تسجيل المواقع المختلفة على الويب المظلم يمكن معالجتها باستخدام تشفيرات رياضية مختلفة تعتمد على خوارزميات صممت خصيصاً لهذا الغرض؛ حيث يتم تبادل لهذه الخوارزميات ولذلك فإنّ الويب المظلم هو المجال الكبير لتبادل تقنيات إنشاء تلك المواقع مع البرمجيات الملحق بها بما يضمن عدم متابعة أي عميل للحكومات لهذه المواقع وكشف المصدر الحقيقي لها؛ لذلك كان لا بُدّ من عمل فهرس وتفاصيل دقيقة لتلك المواقع والتي تتبدل في اليوم الواحد أكثر من مرة؛ لزيادة صعوبة كشفها وتتبعها حيث إنّ عمليات إنشاء المواقع كما أسلفنا تعتمد على خوارزمية عشوائية ولذلك واجهت الحكومة والأطراف العليا صعوبة في تتبع تلك المواقع والإمساك بأصحابها، دأبت الكثير من الحكومات بكل تأكيد على المتابعة المستمرة والولوج إلى المعلومات المنتشرة في الويب المظلم والتي كثيرة منها ما تكون ممنوعة وغير متوفرة لنا في النطاق العام والكثير من هذه المعلومات تندرج من ضمن الآتي:

أولًا: التسريبات الحكومية أو المعلومات المتعلقة بالأنشطة الحكومية المختلفة ونشاطات مجموعة الاختراقات المرتبطة بالفعاليات الحكومية مثل تسريبات الموقع العالمي الشهير «ويكي ليكس».

ثانيًا: معلومات عن الثغرات الأمنية غير المعلنة والرموز البرمجية المختلفة التي تساعد على الاختراق والتي تعتبر مصدرًا لتقنية عالية الجودة للمخترقين والباحثين في مجال الحماية والجريمة الإلكترونية.

ثالثًا: معلومات تقنية أو أسرار صناعية ممنوعة من تداول مثل صناعة العقاقير الممنوعة وغيرها.

رابعًا: وثائق ودراسات غير ممنوعة من النشر لكن أصحاب تلك الدراسات والوثائق يحتاجون لإخفاء هويتهم الحقيقية خوفًا من الملاحقة والتصفية الجسدية.

وينبغي أن نفكر بشكل مهم عن العملات الرقمية المستخدمة في التداول داخل منظومة الويب المظلم هي عملة البيتكوين (bitcoin) والإيثريوم (Etherium) وليبرا (Libra) وغيرها من العملات الرقمية ذات الأهمية المالية لأنّ معظم العمليات المشبوهة تجارية تتم من خلال تلك العملات الرقمية لذلك كانت الحكومات على علم ودراية كاملة بخطورة وأهمية ترك العملات الرقمية في ابتكار وإنشاء اقتصاد موازي لا تريد أي حكومة رأسمالية أو اشتراكية أن يكون له وجود.

4.4 الجايا الرقمية Digital Gaia

لا شك بأن ممارسة الأنشطة غير القانونية مثل ما أسلفنا سابقًا هي أحد المحركات الأساسية لإنشاء شبكة الإنترنت المنظمة أو الويب المظلم؛ حيث يستطيع الكثير من البشر ممارسة جميع الأنشطة الإجرامية التي تتنافى مع الأخلاق ومن خلال استخدام تقنيات مختلفة دون أدنى شيء من الخوف من الجهات القانونية. بالتأكيد هناك بعض المنتديات التي توفر الدعم التقني للكثير من تطبيقات الويب المظلم، المنتديات بشكل عام أيضًا توفر مساحة معينة من خصوصية تبادل المعلومات والأفكار والقدرات الإبداعية لإنشاء المواقع بل وحتى توفير مظلة قانونية مع الهاكر المخترقين للكثير من المواقع الرقمية المتواجدين بكثرة على مستوى العالم؛ ولذلك فإن تتبع تلك المواقع، مما يجعلنا نعتقد بأن التنسيق العالي بين تلك المواقع والمنتديات يكون قلعة حصينة لا يمكن اختراقه. هذا ما يؤسس لوجود ملاحظات آمنة بـ«غياهب ودهاليز» رقمية أو ما أشبه بالمغارات الرقمية التي يلجأ إليها العديد من طلاب الحرية الشخصية ومؤسسي العمليات الإجرامية كذلك وهو

المحرك الأساسي بتأسيس تلك المواقع. طبعًا مع عدم الإخفاق أن هناك بعض الدول المؤثرة في تشجيع إنشاء مواقع على الويب المظلم أمي ترد عليك دولة كوريا الشمالية التي تعتبر المسيطر الرئيسي على عمليات تبادل العملات الرقمية والاتِّجار بالأسلحة والمخدرات وبعض المواد غير المشروعة والتي تساهم تلك العمليات في تمويل برامجها الأخرى مثل البرنامج النووي والبرامج الصاروخية التي تعمل عليها؛ لهذا السبب أيضًا فإنّ هذا العالم يخلق ساحة ألعاب دولية قذرة بين العديد من الأطراف السياسية الإقليمية المتنازعة فعلى سبيل المثال قامت بعض المجموعات من كوريا الشمالية باختراق بعض المواقع اليابانية وتعطيلها من خلال تشفيرات خاصة تم بناؤها وتجريبها في الويب المظلم كان ذلك عام 2017. وبالمقابل قامت بعض العناصر المتخصصة في مجال الأمن السيبراني في اليابان بمهاجمة بعض المواقع التابعة إلى الهاكرز من كوريا الشمالية وتم تعطيل تلك المواقع لأكثر من شهرين؛ لذا من نافل القول إنّ «الديب ويب» هو أشبه بمتجر كبير ومفتوح بشفرات سرية لكل ما هو غير شرعي وغير قانوني ولكن كيف يمكن التعرف على تلك المواقع والربط بينها وبين خريطة ذلك الإنترنت المظلم والصلات الممكنة مع الإنترنت العادي الذي يرزح تحت مراقبة الحكومة.

في صيف عام 2019 أضافت إحدى الشركات الفرنسية تحديثات مهمة على برنامج يتم تصميمه للكشف عن مغارات الديب ويب، واستخدمت أدوات من الذكاء الاصطناعي للتعرف على الكثير من الوثائق والصور مثل ضحايا الاستغلال الجنسي أو الأسلحة المحرمة وصولاً إلى المنتجات المقلدة التجارية وأصبحت هناك أدوات فعالة ومتوفر في يدِ الحكومة باستخدامها؛ لمراقبة متجر الجريمة الويب المظلم؛ لذلك كان من الطبيعي أن تقوم كل الحكومات بكافة تفاصيلها الإدارية والسياسية والاقتصادية والأمنية بتتبع كل مستخدمي الشبكة المظلمة والقبض على من يقومون بأنشطة تعتبرها الحكومات معادية ومضللة لأمنها الوطني والقومي. فاستخدمت الكثير من موارد البنى التحتية الرقمية لمتابعة تلك الشبكة موظفةً العديد من الشركات ذات الخبرة الطويلة في بناء شبكة الرصد الطويل وأنظمة التعقب الفردية الرقمية؛ لصيد المستخدمين لتلك الشبكة. فمهما كان رأينا في الويب المظلم فإنه من زاوية أخرى يمكن أن نعتبرها الملاذ الآمن للكثير من المنظمات الحقوقية كما أسلفنا وكذلك زاوية أمينة لتبادل المعلومات والإرشاد حول انتهاكات تلك الحكومات لحقوق الإنسان وحقوق مواطنيها الأساسية مما يجعل متابعات لك الشبكة بغض النظر عن الأنشطة الإجرامية التي تجري فيها مسألة اختراق خصوصية أخرى. فلولا الويب العميق لما استطعنا رؤية

وتصفح ملايين الوثائق التي قدمها موقع ويكي ليكس ولا ما استطعنا كذلك من رؤية الكثير من الأسرار التي تم إعلانها من قبل سنودن.

قامت بعض الشركات الأخرى بتطوير أسلحة ردع رقمية وهي أشبه بروبوتات إنترنت (Botnets) تم الحديث عنها سابقاً في هذا الكتاب من ضمن فصل الأسلحة الرقمية وهي ماسكات مشخصنة افتراضية تقوم بعملية مسح كافة المحتويات الخاصة بالشبكة المظلمة أو الويب المظلم، وتقوم بعد ذلك بعزل المعلومات وتبويبها وتصنيفها حسب أهميتها باستخدام كلمات دلالية ذكية قابلة للتغيير. إذا اعتمدت الجهات المتطورة في تلك التقنية على أنظمة الذكاء الاصطناعي؛ ولذلك أصبح الويب المظلم ميدان حربٍ فعلي للكثير من الأطراف من ضمنها أطراف حكومية، بلدان، عصابات إلى آخره. وهنا لا بُدّ من الانتباه إلى الأمر، حيث من الممكن حدوث ثورة هائلة في التتبع بالتصنت، سرقة المعلومات بما فيها الأسرار العسكرية والاقتصادية والأمنية الشخصية للأفراد داخل أي مجتمع بل يتعدى ذلك إلى عمليات بيع مباشر لتلك الأسرار لأي جهة كانت أو أي جهة تدفع أكثر! إننا بالفعل أمام يوم قيامة رقمية جديد ولا نعرف إن كنا سنشهد نهايته باختراق أنظمة ومعلومات خطيرة للغاية، وهنا نقصد بها منظومات الأسلحة النووية لبلدان معينة تؤدي في نهاية المطاف إلى تفعيل الضربة النووية بشكل عشوائي وبهذا ستنتهي الحياة على هذا الكوكب من جراء هذه اللعبة.

إنها بالتأكيد من أخطار الألعاب التي يمارسها البشر؛ ولذلك فمن المهم تبيان حقيقة تلك اللعبة وما فيها من تهديد صريح، وواضح بمصير البشرية جمعاء، ولكن هل ستسمع الحكومات ذلك النداء الواضح والجلي قبل فوات الأوان، وقبل أن يصبح التدخل السافر في خصوصيات البشر حقًّا من حقوق تلك الحكومات. ما تبقى لنا من حقوقنا الشخصية هي تلك المساحة التي يتمتع بها في حياتنا في أوقات السعادة أو حتى في أوقاتنا المظلمة نحاول أن نأخذ أكثر قدر ممكن من الخصوصية ولكن يبدو أنه حتى ذلك القدر البسيط والمساحة الصغيرة من الحرية تحاول كل السلطات في هذا الكوكب محاصرتها وتصادرها؛ بحجة حماية الأمن القومي وحماية مكتسبات تلك السلطات، وهذه هي الحجة القديمة المتجددة في مصادرة حقوق الشعوب الأساسية وشرعنة بطش الدكتاتورية الغاشم على الشعوب. ولنا في التجربة الصينية خير مثال حيث الشعب هناك يتمتع بكافة المجالات التقنية المتطورة، وبتكلفة زهيدة نسبيًّا ولكن على حساب لماذا أنها على حساب حريته وقدرته على إثبات وجوده كإنسان حر له مساحته الخاصة في التفكير والإبداع ورفض كل أنواع الديكتاتورية التي

تحاول وأد أحلامه وتطلعاته. لذلك كانت الحكومات من أهم الأطراف التي لا تريد أن يكون الويب المظلم ملاذًا آمنًا لأنشطة بعيدة عن الرقابة المستمرة لها لكن هذا الأمر لن يستمر طويلا وستقوم الحكومات عاجلًا أم آجلًا بالاستيلاء على الويب المظلم والعميق وستكون قادرة على التحكم في بواباته ومساراته الرقمية.

في نهاية عام 2019 اكتشف الباحث السيبراني فيني ترويا وجود معطيات خاصة عن أكثر من 1.2 مليار ملف شخصي على ما يسمى النت المظلم، من دون معرفة مصدرها، بحسب ما نقل موقع «وايرد» الأمريكي. ووفقا للباحث فإن المعطيات تشمل بيانات عن حسابات المواقع الاجتماعية، إضافة إلى نحو 50 مليون رقم هاتف، و622 مليون عنوان بريد إلكتروني، وكلها موجودة على خادم واحد فقط. وتم وصف التسريب بالأمر الكارثي حيث يعتبر أكبر تسريب البيانات الشخصية من مصدر واحد في التاريخ. وتمكن هذه البيانات المسربة، القراصنة، من انتحال شخصيات أصحاب الحسابات بسهولة كبيرة على مواقع الإنترنت، وفقًا لتصريحات الباحث. واكتشف توريا التسريب في أكتوبر رفقة زميل له وهو باحث أيضًا في أمن الإنترنت يدعى بوب دياتشينكو، على موقعين لخدمات المسح على الإنترنت. وقال ترويا إنها المرة الأولى التي يصادف فيها هذا العدد الهائل من الملفات الشخصية، تم جمعها ودمجها مع معلومات ملف تعريف المستخدم في قاعدة بيانات واحدة على هذا الشكل. وعثر رفقة زميله على أربع مليارات حساب تعود لـ 1.2 مليار شخص، دون التوصل إلى معرفة من يقف وراء هذا التسريب الكبير. وأوضح الخبراء في ذلك الوقت أنه لا وجود لخيوط تشير إلى الجاني حتى الآن على أن البيانات قد تم تحميلها أو العثور عليها من قبل جهات مستفيدة أخرى لم يتم التوصل إليها.

الفصل الخامس
الأسلحة في زمن الحرب الرقمية

5.1 الحرب الرقمية

«الهجمات السيبرانية، هي أسلحة مؤثرة،
وقليلة التكلفة وكذلك قابلة للإنكار، وهذا
بحد ذاته أفضل توليفة عظيمة لأي سلاح»

ميكو هيبونين - خبير أمني سايبري

تشير الحرب الإلكترونية (الحرب الرقمية) إلى استخدام بلد ما هجمات رقمية - مثل فيروسات الكمبيوتر والقرصنة - تعطيل أنظمة الكمبيوتر الحيوية في بلد آخر، بهدف إحداث الضرر والموت والدمار في البنى التحتية. ستشهد حروب المستقبل المتسللين يستخدمون رمز الكمبيوتر لمهاجمة البنية التحتية للعدو، والقتال إلى جانب القوات باستخدام الأسلحة التقليدية مثل البنادق والصواريخ. إن عالم الحروب الرقمية هو عالم غامض لا يزال مليئًا بالجواسيس والمتسللين وكبار ممولي ومسؤولي مشاريع الأسلحة الرقمية السرية، تعد الحرب الإلكترونية سمة شائعة وخطيرة بشكل متزايد للنزاعات الدولية والإقليمية. ولكن في الوقت الحالي، فإن الجمع بين سباق التسلح المستمر في الحرب الإلكترونية ونقص القواعد الواضحة التي تحكم النزاع عبر الإنترنت يعني وجود خطر حقيقي من أن الحوادث يمكن أن تتصاعد بسرعة خارج نطاق السيطرة.

لكن كيف تبدو الحرب الرقمية؟الحرب الرقمية تشبه الحروب العادية تمامًا، فكلاهما يتراوح بين مناوشات محدودة إلى معارك كاملة، يختلف تأثير الحرب الإلكترونية حسب الهدف والشدة. في

كثير من الحالات، ليست أنظمة الكمبيوتر هي الهدف النهائي - فهي مستهدفة بسبب دورها في إدارة البنية التحتية في العالم الحقيقي مثل المطارات أو شبكات الطاقة. ضرب أجهزة الكمبيوتر ويمكنك إغلاق المطار أو محطة توليد الكهرباء؛ نتيجة لذلك، هناك الكثير من سيناريوهات الحرب الرقمية الكئيبة المتاحة. ربما يبدأ المهاجمون بالبنوك؛ يومًا ما ينخفض رصيدك المصرفي إلى الصفر ثم قفز فجأة، ممّا يدلُّ على حصولك على الملايين في حسابك. ثم تبدأ أسعار الأسهم بالجنون حيث يغير المتسللون تدفق البيانات إلى البورصة. في اليوم التالي، لا تعمل القطارات؛ لأن الإشارات تتوقف عن العمل، ولا يمكنك القيادة في أي مكان؛ لأن إشارات المرور عالقة باللون الأحمر، والمحلات التجارية في المدن الكبرى تنفذ من الطعام. في القريب العاجل، يمكن تحويل أي بلد إلى حالة من الجمود والفوضى، حتى بدون سيناريوهات يوم القيامة المتمثلة في تعطيل المتسللين لمحطات الطاقة أو فتح السدود المائية الضخمة؛ لإحداث أضرار كارثية.

يرى سيناريو الهجوم السيبراني الأسوأ (case scenario Worst) على الولايات المتحدة أن المهاجمين يجمعون بين الهجمات المدمرة المباشرة التي تركز على البنية التحتية الأمريكية الحيوية ومعالجة البيانات على نطاق واسع. ومع ذلك، لا يزال هناك، لحسن الحظ، بعضُ الأمثلة على الحرب الرقمية في العالم الواقعي، على الأقل حتى الآن. يتم تقريبًا دعم كل نظام نستخدمه على نحو ما بواسطة أجهزة الكمبيوتر، مما يعني إلى حد كبير أن كل جانب من جوانب حياتنا يمكن أن يكون عرضة للحرب الإلكترونية في مرحلة ما، ويحذر بعض الخبراء من أنها حالة «متى» وليس «إذا». السؤال الذي يتوجب طرحه اليوم، إذا كانت هذه الأنواع من الحروب فعالة فلماذا تستثمر الحكومات في الحرب الرقمية بشكل مكثف حتى الآن؟نحن نعتقد أن الحكومات تدرك بشكل متزايد أن المجتمعات الحديثة تعتمد اعتمادًا كبيرًا على أنظمة الكمبيوتر لتشغيل كل شيء من الخدمات المالية (Bank transactions) إلى شبكات النقل (Transportation network)، بحيث يكون استخدام المتسللين المسلحين بالفيروسات أو غيرها من الأدوات لإغلاق تلك الأنظمة فعالاً ومدمراً مثل الحملة العسكرية التقليدية باستخدام القوات المسلحة بالمدافع والصواريخ. فعلى عكس الهجمات العسكرية التقليدية، يمكن شن هجوم إلكتروني على الفور من أي مسافة، مع القليل من الأدلة الواضحة على أي حشد، على عكس العملية العسكرية التقليدية. سيكون من الصعب للغاية تتبع مثل الهجوم بأي قدر من اليقين لمرتكبيها، مما يجعل الانتقام أكثر صعوبة. لكن متى نعتبر السلاح سلاحًا رقميًّا؟ذلكم أن اعتبار أي هجوم عمل من أعمال الحرب الرقمية يعتمد على عدد من العوامل.

وتشمل هذه هوية المهاجم، وماذا يفعلون؟، وكيف يفعلون ذلك؟- ومقدار الضرر الذي يلحقونه. مثلها مثل أشكال الحرب الأخرى، عادة ما يتم تعريف الحرب الرقمية بمعناها الأصيل على أنها صراع بين الدول وليس الأفراد. إذا كان من الأفضل فهم الحرب الإلكترونية على أنها نزاع خطير بين الأمم، فهذا يستثني الكثير من الهجمات التي يتم وصفها بشكل منتظم وغير صحيح على أنها حرب (رقمية) إلكترونية. لا تعتبر هجمات المتسللين الأفراد، أو حتى مجموعات المتسللين، حربًا عبر الإنترنت، ما لم تكن مدعومة وموجهة من الدولة وعلى أعلى المستويات القيادية. ومع ذلك، في عالم الحرب السيبرانية الغامض، هناك الكثير من الخطوط غير الواضحة: الدول التي تقدم الدعم للمتسللين من أجل خلق إنكار معقول لتصرفاتهم هي، مع ذلك، اتجاه شائع بشكل خطير. أحد الأمثلة على ذلك: هم المحتالون عبر الإنترنت الذين يعطلون أنظمة الكمبيوتر الخاصة بالبنك أثناء محاولتهم سرقة الأموال، لن يُعتبروا بمثابة ارتكاب فعل حرب إلكترونية، حتى لو كانوا من دولة منافسة. لكن المتسللين المدعومين من الدولة يفعلون نفس الشيء؛ لزعزعة استقرار اقتصاد الدولة المتنافسة. طبيعة وحجم الأهداف التي تمت مهاجمتها مؤشر آخر. فمن غير المرجح أن يعتبر تشويه موقع شركة فردية بمثابة عمل حرب إلكترونية، لكن تعطيل نظام الدفاع الصاروخي في قاعدة جوية سيكون قريبًا على الأقل.

تعتبر الأسلحة المستخدمة مهمة أيضًا - إذْ لا يمكن اعتبار إطلاق صاروخ على مركز بيانات حربًا إلكترونية، حتى لو احتوى مركز البيانات على سجلات حكومية. واستخدام المتسللين للتجسس أو حتى لسرقة البيانات لا يعتبر في حد ذاته عملاً من أعمال الحرب الإلكترونية، بل سيكون بدلاً من ذلك تحت عنوان التجسس الإلكتروني، وهو ما تقوم به جميع الحكومات تقريبًا! من المؤكد أن هناك العديد من المناطق الرمادية (Grey zones) هنا (الحرب السيبرانية هي في الأساس منطقة رمادية كبيرة جداً على أي حال)، ولكن استدعاء كل قرصنة من أعمال الحرب الإلكترونية أمر غير مفيد في أحسن الأحوال، وفي أسوأ حالاته هو تخويف قد يؤدي إلى تصعيد خطير.

5.2 الحرب الإلكترونية واستخدام القوة

سبب أهمية من؟وماذا؟وكيف؟للحرب الإلكترونية أن تحدث هو أن كيفية الجمع بين هذه العوامل سوف يساعد في تحديد نوع الاستجابة العسكرية التي يمكن لأي بلد القيام بها للهجوم

الإلكتروني. هناك تعريف رسمي رئيسي واحد للحرب الإلكترونية، وهو هجوم رقمي بالغ الخطورة ويمكن اعتباره مكافئًا للهجوم الفيزيائي. للوصول إلى هذا الحد، فإن أي هجوم على أنظمة الكمبيوتر يجب أن يؤدي إلى تدمير أو تعطيل كبير، أو حتى خسائر في الأرواح. هذه هي العتبة الكبيرة لأنه بموجب القانون الدولي، يُسمح للدول باستخدام القوة للدفاع عن نفسها ضد أي هجوم مسلح ويترتب على ذلك أنه إذا تعرضت دولة لهجوم إلكتروني على نطاق واسع، فستكون الحكومة ضمن حقوقها في الرد باستخدام قوة ترسانتها العسكرية المعتادة: الرد على الاختراق بضربات صاروخية ربما. لم يحدث هذا مطلقًا حتى الآن - من غير الواضح تمامًا ما إذا كان أي هجوم قد وصل إلى هذا الحد. حتى لو حدث مثل هذا الهجوم، فلن يُفترض أن الضحية ستضرب بالضرورة بهذه الطريقة، لكن القانون الدولي لن يقف في طريق مثل هذا الرد. هذا لا يعني أن الهجمات التي تفشل في الوصول إلى هذا المستوى لا صلة لها بالموضوع أو يجب تجاهلها: فهذا يعني فقط أن البلد الذي يتعرض للهجوم لا يمكن أن يبرر اللجوء إلى القوة العسكرية للدفاع عن نفسه. هناك الكثير من الطرق الأخرى للرد على الهجوم السيبراني، من العقوبات وطرد الدبلوماسيين، إلى الرد بالمثل، على الرغم من أن معايرة الرد الصحيح على الهجوم تكون صعبة في كثير من الأحيان (انظر استراتيجية الردع السيبرانية). أحد أسباب عدم وضوح الوضع القانوني للحرب الإلكترونية هو أنه لا يوجد قانون دولي يشير إلى الحرب الإلكترونية، لأنه مفهوم جديد. ولكن هذا لا يعني أن الحرب الإلكترونية لا يشملها القانون، بل إن القانون ذا الصلة مجزأٌ ومتناثر وغالبًا ما يكون مفتوحًا للتفسير.

أدى هذا النقص في الإطار القانوني إلى وجود منطقة رمادية (grey area) ترغب بعض الدول في استغلالها، مع استغلال الفرصة لاختبار تقنيات الحرب الإلكترونية بمعرفة أن الدول الأخرى غير متأكدة من كيفية تفاعلها مع القانون الدولي. وفي الآونة الأخيرة بدأت تلك المنطقة الرمادية في التقلص. حيث أمضت مجموعة من علماء القانون سنوات في العمل لشرح كيفية تطبيق القانون الدولي على الحرب الرقمية. شكل هذا العمل أساس دليل Tallinn، وهو كتاب مدرسي أعدته المجموعة ودعمه مركز التميز للدفاع السيبراني التعاوني التابع لحلف الناتو (CCDCoE) ومقره العاصمة الإستونية تالين، والذي يأخذ منه الدليل اسمه. في النسخة الأولى من الدليل إلى الهجمات الإلكترونية النادرة ولكنها الأكثر خطورة، على مستوى استخدام القوة؛ حاولت الطبعة الثانية التي تم إطلاقها بناء إطار قانوني حول الهجمات الإلكترونية التي لا تصل إلى عتبة استخدام

القوة. المستشارون القانونيون للحكومات والجيش وأجهزة الاستخبارات، يمكنهم باستخدام دليل Tallinn حديد ما إذا كان الهجوم انتهاكًا للقانون الدولي في الفضاء الإلكتروني، ومتى وكيف يمكن للدول أن ترد على مثل هذه الاعتداءات. يتكون الدليل من مجموعة من الإرشادات - 154 قواعد - والتي تحدد كيف يعتقد المحامون أنه يمكن تطبيق القانون الدولي على الحرب الإلكترونية، والتي تغطي كل شيء من استخدام المرتزقة السيبرانيين إلى استهداف أنظمة الكمبيوتر في الوحدات الطبية. تكمن الفكرة في أنه من خلال جعل القانون حول الحرب الإلكترونية أكثر وضوحًا، يكون هناك خطر أقل في تصاعد الهجوم. ويبحث الإصدار الثاني من الدليل، المعروف باسم Tallinn 2.0، في الوضع القانوني لمختلف أنواع القرصنة والهجمات الرقمية الأخرى التي تحدث بشكل يومي أثناء وقت السلم، وينظر إلى متى يصبح الهجوم الرقمي انتهاكًا للقانون الدولي في الفضاء الإلكتروني؟.



الصورة رقم (8) شكل يمثل حالة الحرب الرقمية وأدواتها

(المصدر: illustration Army US)

لكن من هي الدول التي تستعد للحرب الإلكترونية؟نحن نعتقد أنه وإلى حد كبير كل أمة لديها المال والمهارات تستثمر في الحرب الإلكترونية وقدرات الدفاع عن الإنترنت، وفقًا لرؤساء المخابرات الأمريكية، فإن أكثر من(30) دولة تعمل على تطوير قدرات هجومية عبر الإنترنت، على الرغم من أن معظم برامج القرصنة الحكومية هذه يكتنفها السرية. وقد أدى هذا إلى مخاوف من أن سباق التسلح السيبراني قد بدأ بالفعل. توجز مذكرات الاستخبارات الأمريكية بانتظام روسيا والصين وإيران وكوريا الشمالية باعتبارها الجهات الفاعلة الرئيسية التي تهدد الإنترنت. لقد حذرت

الولايات المتحدة منذ فترة طويلة من أن روسيا لديها «برنامج سيبراني هجومي متقدم للغاية» وأنها «قامت بهجمات إلكترونية ضارة أو مدمرة، بما في ذلك الهجمات على شبكات البنية التحتية الحيوية». إذْ وضح البنتاجون تصريحًا خطيرًا أنّ الصين تتطلع إلى تضييق الفجوة مع الولايات المتحدة فيما يتعلق بقدرات الحرب الإلكترونية، وحذرت من أن الصين حاولت البحث عن شبكات أمريكية للحصول على بيانات مفيدة في أي أزمة مستقبلية: «المعلومات المستهدفة يمكن أن تمكن جيش التحرير الشعبي» قوات الإنترنت لبناء صورة عملياتية لشبكات الدفاع الأمريكية، والتصرف العسكري، والخدمات اللوجستية، والقدرات العسكرية ذات الصلة التي يمكن استغلالها قبل أو أثناء الأزمة. ومع ذلك، من المحتمل أن الولايات المتحدة لا تزال لديها أهم قدرات الدفاع الإلكتروني والهجمات الإلكترونية. متحدثًا في عام 2016، قال الرئيس أوباما: «نحن ننتقل إلى عصر جديد هنا، حيث تتمتع عدد من الدول بقدرات كبيرة، وبصراحة، لدينا قدرة أكبر من أي شخص، سواء من الناحية الهجومية أو الدفاعية». يأتي جزء كبير من هذه القدرة من القيادة السيبرانية الأمريكية، التي لها مهمة مزدوجة: حماية شبكات وزارة الدفاع الأمريكية وأيضًا إجراء «عمليات الفضاء الإلكتروني العسكري الكامل الطيف من أجل تمكين الإجراءات في جميع المجالات، وضمان حرية التصرف الأمريكية / الحلفاء في الفضاء الإلكتروني وتنكر نفسه على خصومنا». يتكون Cyber Command من عدد مما يطلق عليه فرق Force Cyber Mission.تدافع فرق قوة Cyber National Mission Force عن الولايات المتحدة من خلال مراقبة النشاط الخصم، ومنع الهجمات، والمناورة لهزيمتهم. تقوم فرق قوة سايبر القتالية بإجراء عمليات عسكرية على الإنترنت لدعم القادة العسكريين، بينما تدافع فرق قوة حماية الإنترنت عن شبكات معلومات وزارة الدفاع.

بحلول نهاية السنة المالية 2018، كان الهدف هو زيادة القوة إلى حوالي 6200 شخص متخصص للعمل ضمن فرق يبلغ عددها 133 فريقًا بشكل كامل. يُعتقد أن الولايات المتحدة استخدمت أشكالًا مختلفة من الأسلحة السيبرانية ضد البرنامج النووي الإيراني، وتجارب الصواريخ الكورية الشمالية وما يسمى الدولة الإسلامية، بنتائج متباينة. يعكس الأفضلية المتزايدة التي تضعها الولايات المتحدة على قدرات الحرب الإلكترونية في أغسطس 2017، قام الرئيس دونالد ترامب بترقية القيادة الإلكترونية إلى وضع القيادة القتالية الموحدة، والتي تضع على نفس مستوى مجموعات مثل القيادة الأمريكية للمحيط الهادئ والقيادة المركزية الأمريكية. هذا وتمتلك وكالات أمريكية أخرى مثل CIA وNSA قدرات تجسس عبر الإنترنت وقد شاركت في الماضي في بناء

أسلحة إلكترونية - مثل دودة Stuxnet الشهيرة. صرحت المملكة المتحدة أيضًا علنًا بأنها تعمل في مشاريع الدفاع عن الإنترنت والجرائم وتأسيس بنية تحتية كبيرة للحرب السيبرانية، وتعهدت بالرد إذا هوجمت بهذه الطريقة. في أبريل 2018، أكد مدير GCHQ أن الهجمات الإلكترونية التي شنتها أجهزة المخابرات البريطانية تدعم العمليات ضد جماعة ISIS الإرهابية.

من المحتمل أن تشكل تقنيات القراصنة القياسية الأخرى جزءًا من الهجوم الإلكتروني؛ رسائل البريد الإلكتروني الاحتيالية لخداع المستخدمين في تسليم كلمات المرور أو غيرها من البيانات التي يمكن أن تسمح للمهاجمين بالوصول إلى الشبكات، على سبيل المثال. يمكن أن تشكل البرمجيات الخبيثة والفيروسات جزءًا من هجوم مثل فيروس Shamoon، الذي قضى على محركات الأقراص الصلبة لـ 30000 جهاز كمبيوتر شخصي في شركة أرامكو السعودية في عام 2012. ووفقًا لصحيفة واشنطن بوست، بعد الكشف عن التدخل الروسي في الفترة التي سبقت الانتخابات الرئاسية الأمريكية لعام 2016، أذن الرئيس أوباما بزراعة أسلحة إلكترونية في البنية التحتية الروسية. وقال التقرير «تم تطوير عمليات الزرع من قِبل وكالة الأمن القومي وصممت بحيث يمكن إطلاقها عن بُعد كجزء من الضربة الإلكترونية الانتقامية في مواجهة العدوان الروسي، سواء كان ذلك هجومًا على شبكة كهرباء أو تدخلًا في سباق رئاسي في المستقبل». بعيدًا عن صحة هذه التصريحات ومصداقيتها فإن هذا التصريح يعد توضيحًا مهمًا لنوع الحرب القائمة والمستقبلية بين القوى المتصارعة في العالم.

5.3 فيروس الفدية والحرب الإلكترونية

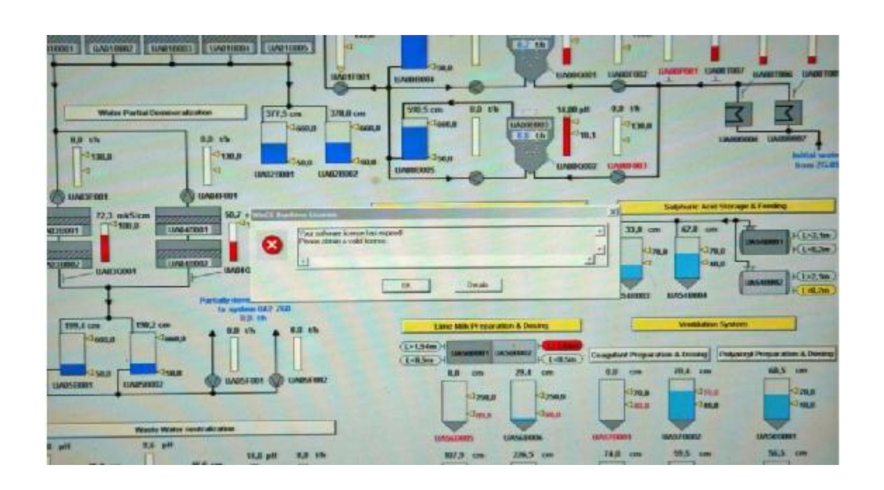
فيروس الفدية Ransomware، التي كانت مصدرًا دائمًا للمشاكل بالنسبة للشركات والمستهلكين، ربما تم استخدامها ليس فقط لجمع الأموال ولكن أيضًا للتسبب في الفوضى. ربما كان أحد أكثر التقلبات غير المتوقعة مؤخرًا استخدام فدية أسلحة مدمرة لتدمير البيانات. ألقت الولايات المتحدة والمملكة المتحدة وعدد من الحكومات الأخرى باللوم على روسيا في اندلاع فدية برامج Not Petya التي تسببت في الفوضى في منتصف عام 2017، حيث وصف البيت الأبيض الحادث بأنه «الهجوم الإلكتروني الأكثر تدميرًا والأكثر تكلفةً في التاريخ». على الرغم من أن الهجوم كان يهدف على الأرجح إلى إلحاق الضرر بأنظمة الكمبيوتر في أوكرانيا، إلا أنه انتشر بسرعة أكبر وتسبب في أضرار بمليارات الدولارات، مما يعكس مدى سهولة تجاوز الأسلحة الإلكترونية لسيطرة صانعيها. بالنسبة لكثير من الناس، فإن عام 2007 هو العام الذي انتقلت الحرب الإلكترونية

من النظرية إلى الفعلية. حيث أعلنت حكومة دولة إستونيا الواقعة في شرق أوروبا عن خطط لنقل نصب تذكاري للحرب السوفيتية حين وجدت نفسها تحت قصف رقمي غاضب ضرب البنوك والخدمات الحكومية دون اتصال بالإنترنت ومع ذلك، فإن هجمات DDoS على إستونيا لم تحدث أضرارًا جسدية، وفي حين أنه حدث مهم، إلا أنه لم يرتفع إلى مستوى الحرب الإلكترونية الفعلية. ومع ذلك، تحقق معلم بارز آخر للحرب الإلكترونية في العام نفسه، عندما أثبت مختبر أيداهو (Idaho) الوطني، عبر اختبار المولد أورورا (Aurora)، أنه يمكن استخدام هجوم رقمي لتدمير الأشياء المادية - وهو مولد في هذه الحالة. وقع هجوم البرامج الضارة Stuxnet في عام 2010، والذي أثبت أن البرامج الضارة يمكن أن تؤثر على العالم المادي.

منذ ذلك الحين كان هناك تدفق مستمر من القصص التي لا تنتهي: ففي عام 2013 قالت وكالة الأمن القومي إنها أوقفت مؤامرة من قبل دولة لم تذكر اسمها - لكن التلميح كان واضحا للصين - لمهاجمة شريحة BIOS في أجهزة الكمبيوتر، مما يجعلها غير صالحة للاستعمال. في عام 2014، وقع الهجوم على شركة Sony Pictures Entertainment، التي ألقى الكثيرون باللوم عليها على كوريا الشمالية، مما أظهر أنه ليس فقط الأنظمة الحكومية والبيانات التي يمكن أن تستهدفها المتسللون المدعومون من الدولة. ربما الأخطر من ذلك، قبل عيد الميلاد مباشرة في عام 2015، تمكن المتسللون من تعطيل إمدادات الطاقة في أجزاء من أوكرانيا، وذلك باستخدام حصان طروادة المعروف باسم Black Energy. في مارس 2016، اتُّهم سبعة من المتسللين الإيرانيين بمحاولة إغلاق سد في نيويورك في لائحة اتهام من هيئة المحلفين الفيدرالية الكبرى. تقوم الدول بسرعة ببناء قدرات الدفاع والهجوم السيبراني، واتخذ حلف شمال الأطلسي في عام 2014 خطوة مهمة لتأكيد أن الهجوم الإلكتروني على أحد أعضائه سيكون كافياً للسماح لهم باستدعاء المادة 5، وهي آلية الدفاع الجماعي في قلب التحالف. في عام 2016، عرفت بعد ذلك الفضاء الإلكتروني بأنه «مجال تشغيلي» ليصبح الإنترنت بذلك ساحة المعركة رسميًا.

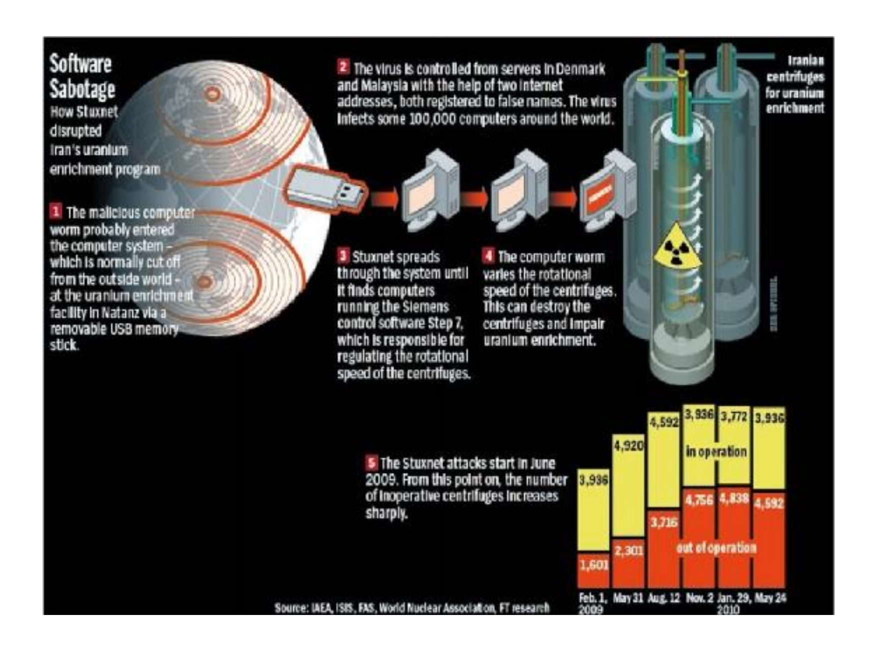
نقاط الضعف في اليوم صفر هي الأخطاء أو العيوب في التعليمات البرمجية التي يمكن أن تمنح المهاجمين إمكانية الوصول إلى الأنظمة أو التحكم فيها، ولكنها لم يتم اكتشافها وحلها بعد بواسطة شركات البرمجيات. هذه الثغرات تحظى بتقدير خاص بسبب عدم وجود طريقة لمنع المتسللين من استغلالهم. هناك تجارة مزدهرة في مآثر يوم الصفر. فهي تجارة مفيدة للغاية للدول

التي تتطلع إلى صنع أسلحة إلكترونية لا يمكن وقفها. يُعتقد أن العديد من الدول لديها أكوام من مخزونات يوم الصفر تستخدم في التجسس الإلكتروني أو كجزء من أسلحة إلكترونية معقدة. شكلت مآثر يوم الصفر جزءًا رئيسيًا من الأسلحة الإلكترونية لشركة Stuxnet. تتمثل إحدى المسائل المتعلقة بالأسلحة السيبرانية، خاصة تلك التي تستخدم مآثر استغراق يوم الصفر، في أنها - على عكس القنبلة التقليدية أو الصاروخ - قابلة للتحليل كسلاح سيبراني وربما حتى يعاد ضبطها وإعادة استخدامه من قبل البلد أو المجموعة التي استخدم ضدها. أحد الأمثلة الجيدة على ذلك هو هجوم WannaCry ransomware، الذي تسبب في حدوث فوضى في مايو 2017. أثبتت الفدية الفظيعة للغاية لأنها كانت مشحونة بضعف في يوم الصفر تم تخزينه بواسطة وكالة الأمن القومي، ويفترض استخدامه في التجسس الإلكتروني. ولكن تم الحصول على الأداة بطريقة أو بأخرى من قبل مجموعة اختراق Shadow Brokers (مدى عدم الوضوح إلى حد بعيد) والتي سربتها بعد ذلك عبر الإنترنت. وبمجرد حدوث ذلك، قام كتاب برمجيات فدية آخرون بدمجها في برامجهم، مما جعله أكثر قوة. هذا الخطر من عواقب غير متوقعة يعني أنه يجب التعامل مع الأسلحة والأدوات السيبرانية - ونشرها - بعناية فائقة. هناك أيضًا خطر إضافي يتمثل في أنه بفضل العالم شديد الارتباط، فإننا نعيش تحت وطأة هذه الأسلحة الي من الممكن أن تنتشر وتسبب أيضًا في فوضى أكبر بكثير مما كان مخططًا له، وهو ما قد يحدث في حالة الهجوم على فيروس الفدية Not Petya الأوكرانية. لكن ما هو فيروس Stuxnet؟إنها دودة كمبيوتر تستهدف أنظمة التحكم الصناعية، ولكنها الأكثر شهرة على الأرجح كونها أول سلاح إلكتروني حقيقي، حيث تم تصميمه لإحداث أضرار مادية. تم تطويره من قبل الولايات المتحدة وإسرائيل (رغم أنهما لم يؤكدا هذا مطلقًا) لاستهداف البرنامج النووي الإيراني. استهدفت الدودة، التي تم رصدها لأول مرة في عام 2010، أنظمة تحكم صناعية محددة من Siemens، ويبدو أنها كانت تستهدف الأنظمة التي تتحكم في أجهزة الطرد المركزي في مشروع تخصيب اليورانيوم الإيراني - مما أدى إلى إتلاف 1000 من أجهزة الطرد المركزي هذه وتأخير المشروع، على الرغم من أن التأثير الكلي على البرنامج غير واضح. كانت Stuxnet دودة معقدة، حيث استخدمت أربعة مآثر مختلفة في يوم الصفر، ومن المحتمل أنها استغرقت ملايين الدولارات من البحث وشهورًا أو سنوات من العمل لإنشائها.



الشكل (9) صورة للواجهة الرسومية لمتحكمات المفاعل النووي الإيراني في محطة نطنز وقد تم اختراقه بواسطة فيروسالـ Stuxnet دودة معقدة شلت البرنامج النووي الإيراني عبر سلسلة تعطيل متعمدة لأجهزة الطرد النووية

في يناير 2010، لاحظ المفتشون في الوكالة الدولية للطاقة الذرية الذين يزورون محطة نطنز لتخصيب اليورانيوم في إيران أن أجهزة الطرد المركزي المستخدمة لتخصيب غاز اليورانيوم قد فشلت بمعدل غير مسبوق. كان السبب لغزًا كاملًا - على ما يبدو - بالنسبة للفنيين الإيرانيين الذين قاموا باستبدال أجهزة الطرد المركزي كما فعل المفتشون الذين يراقبونها. بعد خمسة أشهر من هذه الواقعة تم استدعاء شركة أمان كمبيوتر في بيلاروسيا لاستكشاف سلسلة من أجهزة الكمبيوتر في إيران التي تعطلت وإعادة التشغيل بشكل متكرر. مرة أخرى، كان سبب المشكلة لغزًا. وهذا هو حتى وجد الباحثون حفنة من الملفات الضارة على أحد الأنظمة واكتشفوا أول سلاح رقمي في العالم.



الشكل (9) صورة الانفوجراف لفيروس ال- Stuxnet دودة معقدة شلت البرنامج النووي الإيراني عبر سلسلة تعطيل متعمدة لأجهزة الطرد النووية

يذكر كتاب (Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon) الذي صدر في 2014 كيف تعمل Stuxnet على تخريب أجهزة الطرد المركزي في مصنع ناتانز لمدة عام تقريبًا. حيث تم التلاعب بنسخة مبكرة من سلاح الهجوم بالصمامات على أجهزة الطرد المركزي لزيادة الضغط داخلها وتلف الأجهزة وكذلك عملية التخصيب. أجهزة الطرد المركزي هي أنابيب أسطوانية كبيرة - متصلة بأنابيب في تكوين يعرف باسم «تتالي» - تدور بسرعة تفوق سرعة الصوت لفصل النظائر في غاز اليورانيوم لاستخدامه في محطات الطاقة النووية والأسلحة. في وقت الهجمات، كانت كل سلسلة في ناتانز تحتوي على (164) جهازَ طرد مركزي. يتدفق غاز اليورانيوم عبر الأنابيب إلى أجهزة الطرد المركزي في سلسلة من المراحل، ويصبح «مخصبًا» أكثر في كل مرحلة من مراحل السلسلة حيث يتم فصل النظائر اللازمة للتفاعل النووي عن نظائر أخرى وتصبح مركزة في الغاز. هناك خطر واضح بأننا في المراحل الأولى من سباق التسلح عبر الإنترنت: بما أن البلدان تدرك أن وجود استراتيجية للحرب الإلكترونية أمر ضروري، فإنها ستزيد من الإنفاق وتبدأ في تخزين الأسلحة، تمامًا مثل أي سباق تسلح آخر. هذا يعني أنه قد يكون هناك المزيد من الدول التي تخزن هجمات اليوم صفر، مما يعني أن المزيد من الثغرات في البرامج لا يتم تصحيحها، مما يجعلنا جميعًا أقل أمانًا. والبلدان التي

لديها مخزونات من الأسلحة السيبرانية قد تعني أن الصراعات الإلكترونية قادرة على التصعيد بشكل أسرع. واحدة من المشاكل الكبيرة هي أن هذه البرامج تميل إلى تطويرها سرًّا مع القليل جدًّا من الرقابة والمساءلة وقواعد الاشتباك.

تعتبر الأنظمة العسكرية هدفًا واضحًا: منع القادة من التواصل مع قواتهم أو رؤية مكان وجود العدو هو إعطاء المهاجم ميزة كبيرة ومع ذلك؛ نظرًا لأن معظم الاقتصادات المتقدمة تعتمد على الأنظمة المحوسبة في كل شيء بدءًا من الطاقة إلى الغذاء والنقل، فإن العديد من الحكومات تشعر بقلق شديد من أن الدول المتنافسة قد تستهدف البنية التحتية الوطنية الحيوية. إن أنظمة الرقابة الإشرافية والحصول على البيانات الرقمية (SCADA)، أو أنظمة التحكم المنطقية الصناعية (PLC) - التي تدير المصانع ومحطات الطاقة والعمليات الصناعية الأخرى - هي هدف كبير لتلك الهجمات، كما أظهرت Stuxnet. يمكن أن يكون عمر هذه الأنظمة عقودًا ونادراً ما تم تصميمها مع توفير الأمان كأولوية، ولكن يتم توصيلها بشكل متزايد بالإنترنت لجعلها أكثر كفاءة أو سهولة في المراقبة. ولكن هذا أيضًا يجعل هذه الأنظمة أكثر عرضة للهجوم، ونادراً ما تتم ترقية الأمان نظرًا لأن المؤسسات التي تديرها لا تعتبر نفسها هدفًا. غالبًا ما تُعتبر أنظمة التحكم الصناعية الكبيرة أو الشبكات العسكرية الأهداف الرئيسية للحرب الإلكترونية، ولكن إحدى نتائج ظهور إنترنت الأشياء هي جلب ساحة المعركة إلى بيوتنا.

حيث صرح مجتمع استخباراتي أمريكي (يناير 2017) أن «لدى خصومنا قدرات لتقويض البنية التحتية الحيوية في الولايات المتحدة للخطر فضلاً عن النظام البيئي الأوسع للأجهزة الاستهلاكية والصناعية المتصلة المعروفة باسم إنترنت الأشياء». جميعهم يستخدمون إما للتجسس على مواطني دولة أخرى، أو التسبب في الخراب إذا تم اختراقها. ليست جميع أجهزة إنترنت الأشياء في المنزل وحدها جزء من المعركة بل الأجهزة التي تملأ المستشفيات والمصانع والمدن الذكية الآن كأجهزة بها استشعار وأجهزة أخرى مما يعني أنه يمكن الشعور على نطاق واسع بتأثير انقطاع إنترنت الأشياء. في فصل الجدران الذكية تمت مناقشة مخاطر اختراق شبكة إنترنت الأشياء بتفصيل واستفاضة. لكن كيف لك أنْ تدافع عن نفسك في خضم الحرب الإلكترونية؟علمًا بأنّ ممارسات الأمن السيبراني نفسها التي ستحمي من المتسللين والمحتالين عبر الإنترنت سوف توفر بعض الحماية ضد المهاجمين الإلكترونيين المدعومين من الدولة، والذين يستخدمون العديد من التقنيات نفسها. وهذا يعني تغطية الأساسيات: تغيير كلمات المرور الافتراضية مما يجعل من

الصعب كسر كلمات المرور، وعدم استخدام نفس كلمة المرور لأنظمة مختلفة، والتأكد من أن جميع الأنظمة مصححة ومحدّثة (بما في ذلك استخدام برنامج مكافحة الفيروسات)، وضمان أن الأنظمة تتصل بالإنترنت فقط إذا لزم الأمر والتأكد من أنّ البيانات الأساسية يتم نسخها احتياطيًا بشكل آمن. قد يكون هذا كافيًا لإيقاف بعض المهاجمين أو على الأقل منحهم المزيد من العمل الإضافي للقيام بذلك وهم يتحولون إلى هدف أسهل. حتى إذا لم تكن مؤسستك هدفًا واضحًا للمتسللين بدافع الجشع (من الذي يخترق أعمال الصرف الصحي مقابل المال؟)، فقد تكون أولوية للمتسللين الذين يتطلعون إلى خلق فوضى. ومع ذلك، بالنسبة للأهداف ذات القيمة العالية بشكل خاص، من غير المحتمل أن يكون هذا كافيًا: تسمى هذه الهجمات «متقدمة ومستمرة». في هذه الحالة، قد يكون من الصعب إيقافها عند الحدود وستكون هناك حاجة إلى استثمارات إضافية في مجال الأمن السيبراني: تشفير قوي، مصادقة متعددة العوامل، ومراقبة شبكة متقدمة. ربما لا يمكنك منعهم من اختراق شبكتك، لكن قد تكون قادرًا على منعهم من التسبب في أي ضرر. على مستوى أعلى، تعمل الدول ومجموعات الدول على تطوير استراتيجيات الدفاع الإلكتروني الخاصة بها. أعلن الاتحاد الأوروبي مؤخرًا عن خطط للعمل على خطة للدفاع السيبراني سوف يستشهد بها إذا كانت تواجه هجومًا إلكترونيا كبيرًا عبر الحدود، ويعتزم العمل مع حلف الناتو في تدريبات للدفاع عبر الإنترنت. ومع ذلك، لا تعتبر جميع الدول مثل هذا التخطيط أولوية عالية بشكل خاص. على نطاق أوسع؛ لمنع وقوع حوادث الحرب السيبرانية، تحتاج البلدان إلى التحدث أكثر؛ لفهم أين تقع الحدود وأي أنواع السلوك مقبولة؛ حتى يتم ذلك هناك دائما خطر سوء الفهم والتصعيد.

مثلما تحاول الدول ردع المنافسين عن مهاجمة الأسلحة التقليدية، تعمل البلدان على تطوير مفهوم الردع السيبراني للمساعدة في منع وقوع الهجمات الرقمية في المقام الأول - من خلال جعل تكلفة الهجوم مرتفعة للغاية لأي مهاجم محتمل. طريقة واحدة للقيام بذلك هي تأمين وتدعيم أنظمة الكمبيوتر الخاصة بهم بحيث يصبح من الصعب للغاية - ومكلفة للغاية - لأي مهاجم للعثور على نقاط الضعف. بفضل طبيعة الجبن السويسري للعديد من أنظمة الكمبيوتر، سيظل المهاجمون يتمتعون بالميزة هنا. الخيار الآخر هو فرض التكاليف على المهاجمين من خلال العقوبات أو التحقيقات الجنائية أو حتى التهديد بالرد. في الآونة الأخيرة، تحاول الولايات المتحدة على وجه الخصوص خلق ردع من خلال سياسة التسمية والتشهير، ولا سيما استخدام لوائح الاتهام لتسمية أفراد معينين تعتقد أنهم مسؤولون عن تنفيذ هجمات إلكترونية مدعومة من

قبل الدولة. الدول) الاستمرار في بث وكذب في أنظمة الكمبيوتر من منافسيهم، ويبدو أن الردع السيبراني هو في أحسن الأحوال عمل قيد الإنشاء والتقدم.

5.5 التجسس الإلكتروني

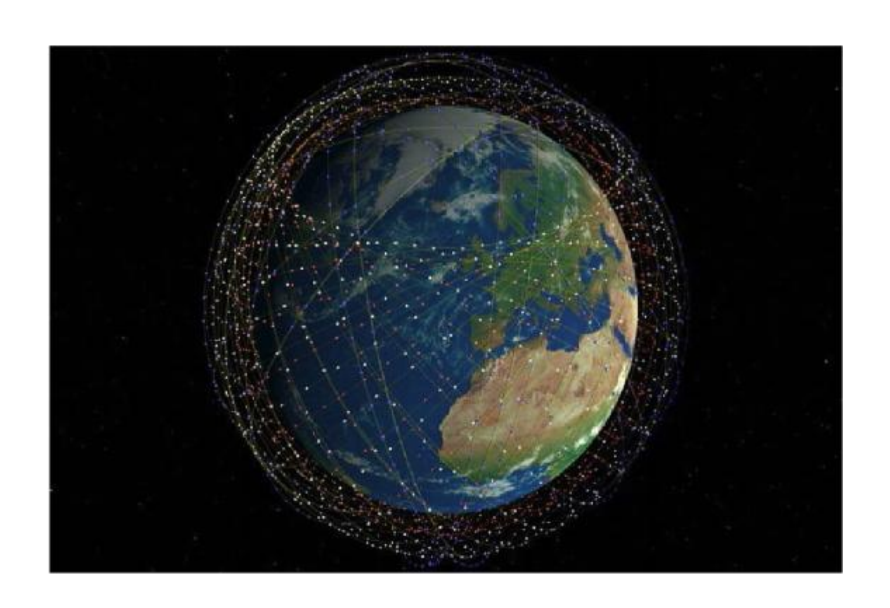
يرتبط التجسس الإلكتروني بشكل وثيق ولكنه منفصل عن الحرب الإلكترونية، حيث يتسلل المتسللون إلى أنظمة وشبكات الكمبيوتر لسرقة البيانات والملكية الفكرية في كثير من الأحيان. كان هناك الكثير من الأمثلة على ذلك في السنوات الأخيرة، على سبيل المثال: الاختراق على مكتب إدارة شؤون الموظفين في الولايات المتحدة، والذي شهد سجلات 21 مليون مواطن أمريكي سرقت، بما في ذلك خمسة ملايين مجموعة من بصمات الأصابع هجمات القرصنة في الفترة التي سبقت الانتخابات الرئاسية الأمريكية عام 2016 المثيرة للجدل وسرقة رسائل البريد الإلكتروني من اللجنة الوطنية الديمقراطية، قالت المخابرات الأمريكية: أن روسيا الهدف من التجسس الإلكتروني هو السرقة، وليس إلحاق الضرر، ولكن يمكن القول: إن مثل هذه الهجمات يمكن أن يكون لها أيضًا تأثير أكبر. ينقسم علماء القانون، على سبيل المثال، حول ما إذا كانت الاختراقات على DNC وما تلاها من تسرب رسائل البريد الإلكتروني قد تكون غير قانونية بموجب القانون الدولي. إنّ الخط الفاصل بين الحرب الإلكترونية والتجسس عبر الإنترنت هو خط واضح: بالتأكيد، السلوك الضروري مشابه لكليهما - التسلل إلى الشبكات، والبحث عن عيوب في البرامج - ولكن النتيجة مختلفة فقط؛ سرقة بدلا من تدمير. بالنسبة للمدافعين، من الصعب تحديد الفرق بين العدو الذي يبحث عن شبكة يبحث عن عيوب يستغلها وبين عدو يبحث في شبكة للعثور على أسرار كما قالها رئيس مجلس الأمن القومي آنذاك روجرز في شهادة أمام مجلس الشيوخ الأمريكي: «عمليات التسلل في البنية التحتية الحيوية للولايات المتحدة - عند النظر إليها في ضوء مثل هذه الحوادث - يمكن أن تبدو وكأنها استعدادات لشن هجمات في المستقبل يمكن أن تهدف إلى إلحاق الأذى الأمريكيين، أو على الأقل لردع الولايات المتحدة ودول أخرى عن حمايتنا والدفاع عنها». نرتبط ارتباطًا وثيقًا الحرب السيبرانية بمفهوم حرب المعلومات؛ أي استخدام المعلومات المضللة والدعاية للتأثير على الآخرين - مثل مواطني دولة أخرى. قد يستخدم هذا التضليل المستندات التي سرقها المتسللون ونشرها - إما كاملة أو معدلة من قبل المهاجمين لتلائم الغرض منها. قد ترى أيضًا استخدام الوسائط الاجتماعية (ووسائل الإعلام الأوسع) لمشاركة القصص غير الصحيحة. بينما يميل الاستراتيجيون الغربيون إلى رؤية

الحرب الإلكترونية وحرب المعلومات المختلطة ككيانين منفصلين، يقول بعض المحللين إن المنظرين العسكريين الصينيين والروسيين يرون أنّ الاثنين مرتبطان ارتباطًا وثيقًا. في الواقع، من الممكن أن يخطط الاستراتيجيون العسكريون الغربيون لهذا النوع من الحرب السيبرانية نتيجة لذلك. تتمثل إحدى الطرق التي تستعد بها الدول للدفاع ضد الحرب الإلكترونية في استخدام مناورات دفاعية عملاقة عبر الإنترنت، والتي تضع «فريقًا أحمر» من المهاجمين ضد «فريق أزرق» من المدافعين. يمكن لبعض من أكبر التدريبات الدولية للدفاع عبر الإنترنت، مثل حدث الدروع المقفلة المدعومة من الناتو، رؤية ما يصل إلى 900 خبير في الأمن السيبراني يشحذون مهاراتهم. في Locked Shields، يتعين على الفرق المدافعة حماية Berylia الصغيرة والخيالية، العضو في حلف الناتو من الهجمات الإلكترونية المتصاعدة من قبل Crimsonia الدولة المنافسة. ليس فقط الجوانب الفنية للحرب الإلكترونية التي تم اختبارها، بل جرى اختبار استراتيجيتهم وصنع القرار في مواجهة هجوم إلكتروني كبير على المنظمات العسكرية التابعة للاتحاد الأوروبي. جرى هذا في اجتماع لوزراء دفاع الاتحاد الأوروبي في أيلول / سبتمبر 2017؛ حين عقدوا اجتماعًا على الطاولة تسمى EU Cybrid، تسمح هذه اللعبة إلى المساعدة في تطوير مبادئ توجيهية لاستخدامها في مثل هذه الأزمة الواقعية، وبإمكاننا اعتبار هذا أول تمرين لإشراك السياسيين في مثل هذا المستوى الرفيع. يجادل البعض بأن الحرب الإلكترونية لن تحدث أبداً؛ ويجادل آخرون بأن الحرب الإلكترونية تجري الآن على قدم وساق. الحقيقة هي بالطبع إنها تجري وبشكل محموم في مكان ما في الوسط. إلى جانب المثال الشهير لعمليات Stuxnet الإلكترونية السيبرانية، ستبقى نادرة للغاية، ولكن هذا المفهوم قد تم استيعابه بالفعل في المجموعة الأوسع من الخيارات العسكرية الموجودة، مثل التقنيات الحديثة الأخرى، مثل الغواصات والطائرات، في الماضي. من المحتمل أن الأسلحة الإلكترونية قد تصبح أيضًا سمة أكثر شيوعًا للمناوشات المنخفضة الكثافة بين الدول لأنها قادرة على التسبب في الفوضى والتدمير والإعاقة التنموية ولكن ليس (كثيرًا) أضرار كبيرة. لكن من غير المحتمل أن يتم خوض حرب أبدًا بأسلحة رقمية بحتة لأنها مكلفة للغاية ويصعب التحكم فيها وذات تأثير محدود. لكن هذا لا يعني أن الحرب الإلكترونية ليست ذات صلة - بل إن بعض أنواع الحرب الإلكترونية ستكون جزءًا من كل اشتباك عسكري من الآن فصاعدًا حتى ولو على نطاق ضيق.

لقد غيّر نظام تحديد المواقع العالمي المجتمع منذ إطلاق أول قمر صناعي، Sputnik 1، في عام 1959. من إعلام الملاحة بالبحار إلى إبقاء الأسلحة «الذكية» على المسار الصحيح، فإن التكنولوجيا لها تطبيقات لا تعد ولا تحصى. يلعب عدد صغير نسبيًّا من الأقمار الصناعية لنظام تحديد المواقع العالمي (GPS)، التي تطير في مدار أرضي على بُعد حوالي 12550 ميلًا، دورًا مهمًا بشكل خاص في المجتمع. في السنوات الأخيرة، كان هناك انتشار للأقمار الصناعية الأقرب إلى الأرض. ومن الأمثلة على ذلك ما يسمى CubeSat، الذي يطير في مدار أرضي منخفض، والذي يتراوح ما بين 110 إلى 1200 ميل تقريبًا. يمكن أن يؤدي توافر الأقمار الصناعية غير المكلفة إلى فتح عدد من المخاطر الأمنية بطريقة مماثلة للطائرات بدون طيار. عند نقطة واحدة، استخدمت الطائرات بدون طيار أو المركبات الجوية بدون طيار في المقام الأول للتطبيقات العسكرية. ولكن مع توفر طائرات أصغر حجماً وأقل تكلفة للجمهور، أصبح عدد مشاكل الطائرات المدنية بدون طيار بالقرب من المطارات والحدائق الوطنية والملاعب، والتدخل في جهود مكافحة الحرائق.

هناك مشاكل أمنية ضخمة تنشأ من التجسس إلى الخصوصية أو {المخاوف} حتى ربما يتم الاستيلاء عليه من قبل مجرمين. قام العديد من البائعين بنشر مواقع وسائل إنترنت الأشياء كوسيلة لتوفير الاتصال بالمناطق الجغرافية البعيدة التي لا تخدمها الشبكات الخلوية أو أنواع الاتصال الأخرى. إن مشكلات الأمن السيبراني المتعلقة بالأقمار الصناعية لنظام تحديد المواقع العالمي (GPS) تشكل مصدر قلق أيضًا. حيث إنّ هذه الأقمار الصناعية تعاني من نقاط ضعف مماثلة مثل أنظمة التحكم الصناعية المتصلة بالشبكات وأجهزة إنترنت الأشياء الأخرى. تعتمد عمليات سلسلة التوريد الروتينية مثل الشاحنات التي تنقل الحاويات إلى الموانئ على أقمار GPS، وكذلك السفن الماخرة عباب البحار. في حين أن هناك شركات مثل Amazon تخطط لوضع أقمار صناعية قادرة على الجيل الخامس في الفضاء، إلا أن الدور الذي ستلعبه الأقمار الصناعية في تمكين نوع الشبكات التي تتميز بسرعة عالية جدًّا وبأمان منخفض للغاية والتي تشتهر بها G5 غير واضح. إذْ يتعين على الأقمار الصناعية أن تدور على بُعد بضع مئات من الأميال لتفادي الاحتراق، وإذا كنت في مدار قريب من الأرض، فهذا يعني أنك إما أن تتحرك بسرعة كبيرة أو أنك في مدار غريب الأطوار تكون قريبًا منك فقط لبضع دقائق في وقت واحد. حتى مع وجود قمر صناعي على بعد 200 ميل فوق الأرض، فإن المسافة تمثل مشكلة. في ميلي

ثانية واحدة، يسافر الضوء بالأميال. «أن أحد معايير G5 هو أن زمن الاستجابة الخاص بك - وقت الاستجابة الكلي لديك - أقل من جزء واحد من الثانية». «لذلك ليس لديك ما يكفي من الوقت للوصول إلى أنظمة الاتصال في القمر الصناعي والعودة، حتى لو لم تكن هناك معالجة على الإطلاق للبقاء تحت هذه العتبة.»



الشكل (10) تدور أقمار ستارلينك starlink على ارتفاع أقل بكثير، مما يقلل من مخاطر النفايات الفضائية غير المرغوب فيه (المصدر: شركة SpaceX).

وهنا يمكن الحديث عن الكثير من سياسة الاختراق التي يعمل على تنفيذها العديد من الأطراف الحكومية والمؤسسات غير الحكومية المعتمدة على برمجيات تجارية أو برمجيات يتم تطويرها من خلال التعاون بين مؤسسات بحثية بين شركات يتم تحويلها من قبل الحكومة كليًّا أو جزئيًّا وبهذا نستطيع أن أستنتج أنه ما أظن فعاليات الاختراق وقت التهديدات الأمنية هي بالأساس يتم التخطيط لها في أدراج المؤسسات الحكومية أو أمر خطير بكل تأكيد ولكن هل يعيد الجمهور العام تلك الجهود بشكل كلي أم هناك نوع من التعميم المتعمدة التي تحاول الحكومة أن تنشرها للجمهور من خلال القنوات الإعلامية والصحفيين التابعين لها. إنّ مسألة اختراق البيانات والتسريبات الرقمية كان لها الأثر البالغ في تدمير كل روابط الثقة ما بين الحكومات وما بين الشعوب وما بين الحكومات فيما بينها بشكل قد يؤدي إلى كوارث سياسية وأزمات اجتماعية لم ينتج عنها سوى فوضى مترامية الأطراف ومعقدة؛ ولهذا لا بُدّ من وقفة جدية في تحليل طبيعة تلك الاختراقات وهل هي ضمن خطة الأمن القومي التي تضعها الحكومة بشكل مستمر؟.

تستمر معالجات الحكومات القصيرة الأجل في تعيين نقاط الاختراق الرقمية ولكنها لا تضع حلولًا طويلة الأمد في معالجتها؛ وبهذا تفقد الحكومات القدرات والمناورة على إنتاج أسلحة مضادة

لتلك الاختراقات. بعض الحلول الحكومية تعتمد على ما يسمى العصفور66 الغاضب وهي طريقة تعتمد على إنتاج حالة دفاعية سريعة التأثير ودقيقة في نفس الوقت ولكنها في حالة أمنية وقتا معينا أي تعتمد الدفع السريع ضد الاختراقات الرقمية وهي لا تتنبه بالهجوم الإلكتروني من خلال الآليات العلمية والأساسية في مكافحة القرصنة والتجسس الرقمي. سنخرج هنا قصة عن أحد البنوك العالمية والذي يتعرض إلى هجمات متزامنة جعلته يفقد الكثير من التحويلات المالية بل أجبرته على إلغاء الكثير من المحافظ المالية والمنتجات الاقتصادية التي كانا ينوي إطلاقها في نهاية العام! لم يكن الفريق الأمني مستعدًا لمثل هذا التهديد ودعا مجلس إدارة البنك معظم أعضاء الفريق الآمنين إلى رفع التقارير الفورية العاجلة حول هذه الكارثة التي تطورت إلى شكل يكون الفريق الأمني مستعدًا هكذا تهديد. ظهر مجلس الإدارة لاحقًا؛ ليعلن أنه ليس بإمكانهم عمل خطة طارئة لمواجهة الاختراق الإلكتروني - كل ما لديهم من مواصفات وتفاصيل تقنية رئيس البنك لكي يقطع وبشكل نهائي كل نقاط الإنترنت المرتبطة بالبنك لمن التحويلات غير القانونية التي قام بها قراصنة الاختراق!

تعود بنا تلك القصة إلى اللحظة الفارقة التي تتخذها الحكومة وقراراتها التجارية لمكافحة هذا النوع من الاختراقات الرقمية حيث لا توجد في خطة أي حكومة خطة الطوارئ محكمة ولا مجموعة الطوارئ لمواجهة هذا الخطر الإلكتروني وكل ما يتداول عن وجود قوة دفاعية وآلية قيادة وإدارة هذا النوع من الأزمات هي في الحقيقة محض إشاعات. نعود إلى إدارة البنك بهذه الحادثة الكبيرة حيث قام محلل الأمن السيبراني وبطريقة مترددة بتصريح مثير مفاده أن أي شخص من أعضاء الفريق الأمني لا يستطيع حماية هذا البنك العالمي من الهجوم! فاقترح أحد العاملين في مجال الأمن المعلوماتي خلال تلك الجلسة النارية في صناعة جدار من الدخان وهو ما يعرف اصطلاحا بتعمية خوادم شبكة الإنترنت المرتبطة بالمؤسسة التي تخدمها وهو من الحلول الخطيرة التي يلجأ إليها خبراء الأمن المعلوماتي في نهاية المطاف للتقليل من خسائر الاختراق الرقمي. بقي أن نعرف أن نظام الاختراق الأمني يتم عبر عمليات وخطوات معقدة تتضمن الكثير والعديد من اللوغاريتمات الرياضية يتم إنشاؤها وكتابتها من قبل خبراء متخصصين في هذا المجال ومنهم لديه خبرة طويلة في عمليات اختراق شبكات الإنترنت في المؤسسات الحكومية كما أسلفنا في فصل الغياب الرقمية أن الكثير منهم يتم استئجار خدماتهم عن طريق الويب المظلم. وهناك في تلك الزوايا المظلمة يتم عقد الصفقات وتحديد عقود هؤلاء الخبراء من قبل عناصر أمنية ومخابراتية أو متعاقدين في سبيل إنجاح تنفيذ مثل هذه الهجمات! كيف سيكون شعورك حيال احتمال شراء سيارة

لم يتم اختبارها؟أو عن السيارة التي سجلتها كان لها سجل سيء في اختبار التصادم على سبيل المثال؟

الفصل السادس

ما بعد الفوضى (Postapocalyptics)

6.1 شريعة الافتراس

«أن تعيش في ديستوبيا لا يحكمها سوى
شريعة الافتراس والبقاء فقط بأي ثمن، هو
المستقبل الذي رسمه الطمع الذي نراه الآن»

ـ المؤلفين

ربما تبدو شريعة الافتراس القادمة فانتازيا غريبة لكن الواقع يؤكد أن الكثير سوف يحدث بعد الخراب العظيم لكل الأنظمة الرقمية والشبكات الإنترنت التي تسيطر على كل شيء الآن من رحلات الطائرات وشبكات التوزيع المياه والمجاري وشبكات الكهرباء ومعظم أنظمة توليد الطاقة والسدود من خلال هجوم منظم من قِبل دول ضد دول أخرى أو من قبل عصابات محترفة تعمل على إسقاط أنظمة حكم ما لها علاقة عدائية مع بعضها البعض. إن هذا السيناريو من الممكن أن يكون حاضرًا بعد الحروب الكبرى التي ستحدث بين القوى العالمية المتنافسة أو بعدها أو بعد الخراب. الخراب لن يكون في الأنظمة الرقمية وحسب مع وجود سبب وجيه هو أن كل أنظمة الطاقة الكهربائية قد تكون اختفت تماما من الوجود فليس من الممكن تشغيل أي أجزاء الكمبيوتر بدون تلك الطاقة أو بوجود الشتاء الطويل بفضل العواصف النووية. هذه التغيرات سوف تنشب من خلال القصف المتبادل بالاعتداء النووية المختلفة بين الدول ذاتها بما يطلق عليه حروب القوى/ الموارد أو حروب الموارد /الموارد أو حروب القوى/ القوى؛ ولذلك فإن حتى الطاقة الشمسية لن تكون ذات جدوى في حال غطى الأرض ذلك الشتاء النووي الطويل.

لقد اختفت الآن إلى غير رجعة ولن تعود مرة ثانية تلك الحياة ونوستالجيا نسجتها أدمغتنا؛ لأن الأرض غير الأرض التي أصبحت بلون برتقالي باهت كأنها صحراء المريخ. والسماء غير السماء التي أصبحت رمادية قاتمة ملبدة بالغيوم القاتلة لن يستطيع أي إنسان أن يتعايش مع هذا الجحيم في ذلك الأتون الكبير لن يتبقى للخصوصية أي معنى، لأن من كان يعتبرها منجما للذهب يتمكن من خلاله من جمع المعلومات وبناء شبكات التسويق في مختلف المنتجات التي يريدها المستهلك قد انتهى نظامه وانتهت معه تلك السطوة والسُلطة! كل ذلك قد اختفى من الوجود ولم يتبقَ للقليل من السكان الذين نجوا من تلك الحروب المدمرة إلا البحث عن لقمة يسدون بها رمقهم وتحميهم من الجوع الذي سيفتك بهم عاجلًا أم آجلاً. أولئك الأفراد غارقين في الظلام ينظر بعضهم لبعض كل يفكر في الماضي الذي كان. الحياة حتى تلك الموجودة عبر وسائل التواصل الرقمية بكل ما فيها من ذكريات وأحبة وأصدقاء. ينظر الناس إلى بعضهم البعض يترقبون تلك الشوارع المقفرة تحتضن بعض أعمدة الكهرباء والإنارة ولكنها أصبحت ذكرى لما كانت تسمى حضارة إنسانية! ربما كان ذلك العبث المستمر بمصائر البشر والشعوب هو الحافز الذي أطلق إشارات حروب النهاية التي جلبت معها الويل والمستقبل المظلم للبشرية ككل. كان الجميع في غفلة يلعبون أيضًا في مصائرهم وحرياتهم الشخصية من خلال حكومات رجعية استبدادية تسلطت عليهم باسم القانون تارة وباسم الديمقراطية تارة أخرى. وخلال تلك الأنفاق الغريبة تتمكن تلك السلطات من إحكام سيطرتها على مصائر الشعوب وتحققت نبوءة جورج أورويل بسيادة الدكتاتورية والسلطة الغاشمة حتى أصبحنا مثل قطيع الأغنام لا إرادة حرة ولا استقلال ذاتي. لقد أصبحنا مجرد أرقام عند الشركات تتلاعب بها كيفما تشاء من خلال لوغاريتمات رياضية ولكن بعد ذلك سوف تكون تلك الأرقام مجرد ذكرى تتلاشى شيئا فشيئا ولم يتبقَ منها إلا الظلال. كأنّ شريط الذكريات يستعرض ببطء شديد في رأس ذلك الرجل الذي يحدق في منظر الجزء المهدوم من جسر المدينة والتي أصبحت هي الأخرى أطلالاً بشعة. لم يتحمل الكثيرون صدمة سقوط الحضارة وتلاشي المدنية. وسقط بينهم الكثير من الجوع ونقص الرعاية الصحية في السنوات الأولى من تلك الكارثة العالمية. يتذكر رجل آخر في زاوية بعيدة، منشورات شبكات التواصل الاجتماعي الأخيرة وكان من بينها تلك الرسائل العاجلة التي انتشرت بين المستخدمين وكان عنوانها سقطت شبكات الطاقة الناس تجري مسرعة في الطرقات على غير هدى، هناك فوضى في الطرق، السلطات تفقد السيطرة، الناس في هلع، هناك

حوادث سقوط الطائرات بشكل فجائي، انفجارات عشوائية في المدن، تفشي أوبئة مخيفة وسريعة الانتشار.

كان Twitter قد امتلأ بالـ تريندات trends والموسومات hashtags التي تحدث الناس عن الكوارث والحوادث المفاجئة التي تتوالى كل ثانية والفوضى التي أحدثتها بين السكان في كل بقاع العالم هذا هو سيناريو يوم القيامة (doomsday scenario) التي تحدثت عنها الكثير من الأديان ولكن بسردية أخرى لا تتحرك فيها الجبال ولا تغيض الأنهار ولا تغضب البحار ولكنها سردية يوم القيامة الرقمي الذي يحمله معه الفوضى الأبدية ونهاية عصر التمدن الذي صنعه الإنسان من خلال الجشع والطمع الذي حوله السلطات إلى أدوات القمعية وتجي السيئة على مواطنيها مما ولد ردود فعل من جانب الكثير الذي يود أن يتحد الحكومة وسلطتها. بالتأكيد لن يكون هناك وقت لوضع الملامة على هذه الجهات أو تلك؛ لأنَّ تلك الجهات بأجمعها ستختفي وستكون السطوة والقوة لمن يستطيع أن يتكيف مع الأحداث الجهنمية التي سوف تقبع فيها الأرض حقباً طويلة!

لا تستغرب أيها القارئ من هذا السيناريو، لأنه أقرب إلينا من أي وقت مضى. ربما الأجيال الحاضرة لن تعيشه لكن بكل تأكيد فإن الأجيال القادمة ستكون محور هذا السيناريو الأسود. هنالك الكثير من الفلاسفة والمفكرين الذين حذروا مرارًا وتكرارًا من سطوة جديدة للقوَى العالمية باستخدام بيانات مواطني الدول حتى توقع سلوك هؤلاء المواطنين بالاعتماد على تلك البيانات المسروقة منهم بما يجعلنا في عصر جديد هو مزيج بين الأوتوقراطية الاشتراكية وبين الرأسمالية المحتكرة! هذا النوع الهجين من نظام الحكم لن يأتي بسهولة ولا يتقبلها الناس والجمهور بأريحية؛ لأن الإنسان بطبعه لن يسمح لأحد أن ينتهك حريته والمقصود هنا حرية بياناته الشخصية وحرية الحفاظ على أسراره! لكن النظام الجديد لن يسمح بهذا وستكون هناك الكثير من مراحل المعارك والاصطدام بين الحكومة وبين المواطنين ستدور في نهاية المطاف إلى مواجهة مع الأنظمة الأمنية. قد يستخدم المواطنون فيها كل الوسائل لإسقاط الحكومة ومن ضمنها عمليات استهداف مراكز القوى والترسانة العسكرية في تلك الحكومات والتي بطبيعة الحال تستخدمها الأخيرة لترهيب دول أخرى أو مواطنيها. وهناك الكثير من الأمثلة على حركات التمرد الداخلية التي حدثت في دول رأسمالية و«ديمقراطية» ومنها الهجوم الكيميائي الذي شنته مجموعة الشمس (أوم شنريكيو المحظورة - بقيادة شوكو اساهارا) في اليابان ضد مترو الأنفاق وتسبب بخسائر بشرية فادحة. إذاً فالصدام مؤجل

بين أنظمة الحكم الجديدة وبين المواطنين الناقمين على سرقة حاضرهم ومستقبلهم، سنرى قريباً ذلك الاشتباك المأساوي ولن تكون تلك اللحظات سعيدة لمستقبل البشر بل ستكون الحد الفاصل بين الحياة وبين الموت والهلاك البطيء لمعظم الحضارة البشرية.

إنّ سردية الطمع والتسلط لن تنتهي إلا بأتون الشر المستدام ولهذا معنى كبير وعميق وصلنا إلى تفكيكه بشكل كلي تقريباً في الفصول السابقة من هذا الكتاب، والتي أشارت بوضوح أنه من غير المبرر للسلطات أن تخترق آخر حصون الحريات التي يتمتع بها الإنسان مهما كان الثمن. والسبب وراء ذلك، أنها الملاذ الأخير لضميره ووعيه الحضاري الذي راكمه على مدى آلاف السنين مرتحلاً معه في كل منعطفات التاريخ. حاملاً معه مخاضًا في الكثير من المحن والكوارث وانتصر عليها بنجاح ولكن هذا التحدي الأخير لن يمر بسهولة؛ لأن حضارتنا قد امتلكت أسلحة الدمار الشامل وهي الخطر المحدق بكل هذا الكوكب. كل تلك التصرفات البراغماتية والتي ستؤدي إلى كوارث لا حصر لها هي نتيجة عناد وتعنت غريب من قبل تلك الحكومات التي تؤثر على السماح لأي شركة التجارية بالتعاون معها في سبيل سرقة بيانات شخصية لمواطنيها واستخدامها لاحقًا ضدهم بممارسة أقل ما يقال عنها بأنها إجرامية وتخترق كل الدساتير الديمقراطية التي تتبجح تلك الحكومات باتباعها والسير على نهجها والحقيقة غير ذلك. لكن في الجهة المقابلة هناك الكثير من الطبقات السكانية التي توائم مع توجهات الحكومة وتمشي عكس التيار العام لباقي المواطنين وهؤلاء إما تم استغفالهم أو هم بالأساس ومدلجين بشكل أعمى لأتباع تلك الحكومات الكاذبة وبتوافق تام.

يوفر شعار الواجهة لساعة العلماء الذرية رمزًا ملموسًا القدرة البشرية على تدمير نفسها في الحرب النووية. في فجر العصر الذري - النووي، عندما أسس أينشتاين وغيره من العلماء المعنيين النشرة الدولية العلمية في عام 1947، تم تعيين ساعة يوم القيامة الرمزية الخاصة بها من الساعة السابعة إلى منتصف الليل - إلى أي مدى كان العالم أقرب إلى الدمار. كلما كانت الأحداث السياسية قد أوصلت الحضارة إلى شفا الموت - مثلما حدث عندما اختبرت الولايات المتحدة والسوفييت قنابلهم الهيدروجينية الأولى - اقتربت عقارب الساعة من الساعة إلى منتصف الليل. من عام 1991 إلى أوائل عام 1998، تراوحت إعدادات الساعة من أربع عشرة إلى سبع عشرة دقيقة حتى منتصف الليل (أقلها تهديدًا منذ تأسيس النشرة)، والتي تمثل رمزًا لتنفس الصعداء العظيمة في العالم وجعله في حالة من الارتياح، حيث إننا لم نعد على حافة الحرب. ومع ذلك، على الرغم من

العلاقات الدولية الأكثر استرخاءً، لا تزال الكارثة النووية تمثل خطراً محتملاً شاخصاً في كل النقاشات الدولية والعالمية. في يونيو 1998، إدراكًا لهذه الحقيقة والاعتراف بالاختبارات المشؤومة للأجهزة من قبل الهند وباكستان، نقل مجلس إدارة النشرة يد ساعة يوم القيامة إلى تسع دقائق حتى منتصف الليل. في آخر تحديث لها في يناير من هذا العام اقتربت تلك الساعة من دقيقتين حتى منتصف الليل بسبب تفشي فيروس كورونا في الصين من مدينة يوهان الصينية. ومنذ نهاية عام 2019 بدأت المرحلة الأكثر خطورة من كورونا 19 - COVID. حيث بدأت أوروبا بطرح تطبيقات رقمية للتحكم في انتشار الفيروس التاجي 19 - COVIDلكنها تواجه تحديًّا كبيرًا، جعلها متوافقة مع قواعد خصوصية البيانات للاتحاد الأوروبي الصارمة. إذ أن تطبيقات الجوّال لتتبع تحركات الأشخاص وجهات الاتصال يمثل مشكلة شديدة الحساسية في أوروبا. في وقت سابق، أصدرت هيومن رايتس ووتش وأكثر من 100 منظمة أخرى دعوة مشتركة للحصول على ضمانات بشأن كيفية استخدام الحكومات للمراقبة الرقمية، بما في ذلك بيانات موقع الهاتف المحمول، لمكافحة الوباء. منذ بداية جائحة 19 - COVID، كان مطورو التكنولوجيا يبحثون عن طرق لتتبع انتشار الفيروس التاجي الجديد والحدّ منه. استخدمت كل من كوريا الجنوبية والصين وسنغافورة التطبيقات كجزء من استجابتها للصحة العامة لـ 19 - COVID، لكن النقاد أثاروا مخاوف بشأن الخصوصية والاستخدام غير القانوني للبيانات. تصدرت إسرائيل عناوين الصحف في مارس 2020 عندما أعلنت أنها ستبدأ في تعقب المواطنين المصابين واتصالاتهم باستخدام تكنولوجيا مراقبة الهاتف المخصصة تقليديًّا لعمليات مكافحة الإرهاب.

وتبعتها تركيا في نفس السياق السيبراني حيث إنها ستستخدم تطبيق الهاتف الذكي لتتبع المرضى المصابين واتصالاتهم. إذا وجد شخص ما أنه إيجابي لـ 19 - COVID - أو شخص كان على اتصال وثيق مع أحدهم - يكسر الحجر الصحي الخاص به، فسيحصل على رسالة نصية آلية أو مكالمة هاتفية تطلب منه العودة إلى المنزل. إذا تجاهلوا التحذير، سيتم تنبيه الشرطة تلقائيًّا. في ألمانيا على سبيل المثال، يعمل أكثر من مئة باحث من ثماني دول أوروبية - مشروع تتبع الخصوصية الأوروبية للحفاظ على القرب (PEPP - PT) - على العمود الفقري لتطبيق مفتوح لأي دولة لاستخدامه ويكون متوافقًا مع قوانين الخصوصية في الاتحاد الأوروبي. أما في جانب آخر من ضرب مفهوم الخصوصية قامت الحكومة الفرنسية في تبني تطبيق يسمى StopCovid، والذي من شأنه، على أساس طوعي واستخدام تقنية Bluetooth، إبلاغ الأشخاص إذا كانوا على اتصال

مع شخص مصاب. بينما يحاول السياسيون الترويج للفكرة بصورة متكررة وغريبة ومستمرة في كل وسائل الإعلام، يلاحظ الخبراء أن حصة كبيرة من سكان البلاد ستحتاج إجباريًّا إلى الاشتراك وتنزيل هذه التطبيقات على هواتفهم لكي تكون فعالة. سيكون التحدي الذي يواجه المطورين والسلطات هو إقناع الناس بأن خصوصيتهم محمية بما يكفي وهذا الأمر لا يعدو كونه إبرة تخدير للقادم الأسوأ وهو السيطرة الأمنية الكلية للحكومات على الشعوب.

لنذهب للجانب الآخر من الأرض هناك حيث أولى الحالات الإصابة بهذا الوباء العالمي في الصين فمع اندفاع هونغ كونغ والولايات القضائية الأخرى لاحتواء الفيروس، يتم نشر عدد كبير من التكنولوجيا لمراقبة تحركات الأفراد. مع استخدام أفراد الشرطة والجيش أيضًا لفرض الحجر الصحي وحظر التجول وتدابير التواصل الاجتماعي - يُزعم أن إحدى الحالات الأخيرة في كينيا أدت إلى وفاة طفل يبلغ من العمر 13 عامًا - ينتشر الوباء على الحريات الشخصية والخصوصية، مما يمنح السلطات يخشى البعض أنهم قد يحجمون عن الاستسلام بمجرد انتهاء التفشي. في هونغ كونغ أيضًا، حيث العلاقة مع الحكومة المركزية في الصين مشحونة بالفعل نتيجة للاحتجاجات المستمرة التي بدأت العام الماضي بسبب مشروع قانون تسليم المجرمين المحجوز الآن، قوبلت التدابير التي تراقب تحركات المواطنين ببعض القلق وخاصة أن السلطات الصينية استخدمت تقنيات الحجر الصحي كأسلوب لإنهاء الاحتجاجات العنيفة كما خططت له ولكن اعتماداً على تلك الجائحة الوبائية التي تعتبرها بعض الأنظمة الديكتاتورية والأوتوقراطية نعمة نزلت من السماء.

هونغ كونغ كانت فريدة من نوعها في استخدام التكنولوجيا لمراقبة الأفراد الخاضعين للحجر الصحي، حيث يتم استخدام تدابير مراقبة أكثر تطفلاً. في فبراير 2020 في أوج الموجة الأولى من جائحة كورونا، تم إطلاق تطبيق مدعوم من الحكومة الصينية لتسجيل اتصالات وثيقة بالمرضى والمواطنين الذين كانوا على تلامس مباشر مع أي مريض أو مشتبه حمله للفيروس. وهذا التطبيق المثير للجدل، الذي تم استعماله من قبل الشخص بتسجيله رقم هاتف الشخص، يجمع أيضًا الأسماء وأرقام الهوية الوطنية لكل فرد وهو انتهاك صريح للخصوصية وجمع مستمر لكل المعلومات التي تريدها الدولة والنظام من المواطن. في كوريا الجنوبية، التي وفقًا لدراسة أجراها مركز بيو للأبحاث العملياتية والسيبرانية، والتي لديها أعلى نسبة من ملكية الهواتف الذكية في أي اقتصاد متقدم، أعلنت البلاد عن «الحرب» على تفشي المرض بطريقة سريعة وقوية. حيث أقرّت تعليمات مشددة تحظر على المسافرين الأجانب الذين لا ينزلون تطبيق

الحجر الصحي بتفويض من الحكومة من الدخول إلى البلاد حتى لو كان للترانزيت فقط. التجربة الكورية الجنوبية كانت تعتمد على إبقاء الجمهور على اطلاع تام بتحديثات التفشي ومخاطر الإصابة بالكشف العلني والشفاف عن المعلومات في الوقت الفعلي سمة أساسية في استجابة الحكومة لأزمة COVID - 19. تنشر الكيانات الحكومية المركزية والمحلية معلومات خاصة بالمنطقة عبر تنبيهات الطوارئ المتنقلة والتطبيقات والمواقع الإلكترونية والمنصات الرقمية الأخرى، ناهيك عن أن الإحباطات اليومية يتم تسليمها للمواطنين من خلال القنوات الإعلامية التقليدية من قبل المراكز الكورية لمكافحة الأمراض والوقاية منها (KCDC). ولقد جاءت تلك السياسات بنتائج مهمة ومبهرة على الصعيد العمليات للسيطرة على الجائحة ولكن بثمن أكيد يعرفه الجميع وهو السيطرة الحكومية الكاملة بكل معلومات الشعب الكوري الجنوبي وبشكل يشبه إلى حد كبير ما يحدث في جارتها الشمالية. وهي الدولة الديمقراطية التي كانت تتبجح بأنها النموذج الأمريكي الليبرالية وحقوق الإنسان في شمال غرب الباسيفيك وشبه الجزيرة الكورية.

باستخدام نظام التحذير العام الكوري القائم على خدمة البث الخلوي، ترسل السلطات الحكومية رسائل تنبيه مخصصة للطوارئ في وقت واحد إلى ملايين مستخدمي الهواتف المحمولة على مستوى المدينة والمنطقة. تتميز هذه الرسائل بتحديثات الحالة بشأن نتائج المسح الوبائي، بما في ذلك تفاصيل الحالات المؤكدة مؤخرًا، ووقت ومكان «نقاط الإصابة» التي زارها هؤلاء المرضى. تدير وزارة الداخلية والسلامة (MOIS) نظام الإنذار العام بالتعاون مع الوكالات الحكومية ذات الصلة مثل إدارة الأرصاد الجوية الكورية والحكومات المحلية الـ 17 في كوريا ومزودي شبكات الهاتف المحمول وشركات تصنيع الهواتف المحمولة لضمان حلول سريعة وموجهة ومستندة إلى الميدان. ومن خلال خطوات مدروسة حكوميًا للسيطرة على الوباء يتم وضع الأشخاص الذين يعانون من أعراض ينتظرون نتيجة الاختبارات الطبية، أو أولئك الذين ينتظرون نتائج الاختبار بدون أعراض، على حجر صحي إلزامي وفقًا لأمر رسمي من السلطات الصحية. في استجابة عاجلة لانتهاكات هذه الأوامر التي أسفرت عن ارتفاع كبير في عدد الإصابات، طورت MOIS تطبيقًا للجوّال كأداة إنفاذ لمراقبة حركة الأشخاص المحاصرين على أنفسهم بشكل فعال. يجب أن يوافق المستخدمون على جمع معلوماتهم الشخصية واستخدام معلومات GPS. يمكن طلب خدمات الشرطة إذا تم اكتشاف مغادرة الأفراد لموقع الحجر الصحي المخصص لهم، أو حتى تغريمهم أو سجنهم وفقًا لقانون مكافحة الأمراض والوقاية منها.

يعمل التطبيق أيضًا كقناة للإبلاغ عن الأعراض التي تم تشخيصها ذاتيًّا، ويوفر إرشادات للحجر الذاتي ومعلومات الاتصال للمسؤول الحكومي المسؤول عن المراقبة.

وبينما تتسابق الدول لمراقبة تفشي المرض واحتوائه، يقول الخبراء إن حقوق الإنسان معرضة لخطر جسيم، وكثير من الأشخاص مستعد للتخلي عن حقوقه المدنية من أجل احتواء الوباء. وعلى العموم، فإن الناس على استعداد لتحمل طرق المراقبة المتطفلة بسبب مناخ الخوف فيما يتعلق بـ COVID - 19. في ألمانيا، على سبيل المثال، طالب عدد من الناس بفرض حظر تجول عندما رأوا أن الآخرين لا يزالون يواصلون الاجتماع وحتى الاحتفال في الحدائق العامة. فهؤلاء الناس سوف يتخلون بشكل طوعي عن الخصوصية من أجل السماح باتخاذ تدابير لتتبع ورصد انتشار الفيروس، على أمل العودة إلى الحياة الطبيعية التي كانت عليها من قبل. وصفت مجموعة الخصوصية الدولية للدفاع عن الحقوق نشر قوانين الطوارئ الأخيرة والتتبع الإلزامي وأدوات المراقبة الأخرى بأنها «اعتداء صارخ على حريات الناس لم يسبق لها مثيل في نطاقها العالمي».

أحد الشواغل الرئيسية التي تحتفظ بها العديد من جماعات حقوق الإنسان هو أن مثل هذه التدابير قد تكون شيئًا ما هو حصان طروادة، وتطبيع المراقبة المستقبلية وتمهيد الطريق للاستخدام بدوافع سياسية أبعد من ذلك. هناك عاملان غالبًا ما يشاهدان في صنع السياسات العامة يمكن أنْ يعملا جنبًا إلى جنب حتى يمكن تعزيز السلطة السياسية. إحدى هذه الفرص هي الفرصة التي تتيحها الأزمة لخلق سياسات جديدة تفضل القيادة أو حلفائها أو ناخبيها. وتمكن COVID - 19 الكثير من القادة في العديد من البلدان من سَنِّ سياسات بِاسم الاستجابة السريعة والمؤثرة للمرض الذي قد تكون عادة لا تكون قادرة على الحصول على الموافقة التشريعية في ظل الظروف الطبيعية وحتى الكارثية الكبيرة. أما العامل الآخر فهو إضفاء الطابع المؤسسي، الذي يسمح لهذه السياسات التعسفية بالبقاء في مكانها حتى بعد انتهاء المشاكل التي تم تطويرها من أجلها. وهذه المواقف ليست سوى غيض من فيض افتراضي من الحوادث الأمنية التي يتم إنشاؤها الآن مع تغير الوباء العالمي من الطريقة التي تعمل بها أمريكا (ومعظم العالم) الآن. نحن نواجه تسونامي ظاهريًّا من مشكلات الإنترنت المتعلقة بهذه التغييرات الهائلة التي تحدث حاليًا للناس والعمليات والتكنولوجيا. في ختام الأمر يعتقد معظم الخبراء أن مؤسسات القطاعين العام والخاص والحكومة ستحتاج إلى معالجة العديد من انتهاكات البيانات والخصوصية نتيجة

للانتقال الاستثنائي إلى العمل في كل مكان تقريبًا من المنزل في غضون أيام قليلة ودون الكثير من الوقت للتخطيط الصحيح. وتلك الانتهاكات للخصوصية المالية أو الاقتصادية والعلمية سيكون لها تبعات كبيرة حتى بعد انتهاء أزمة الجائحة.

6.2 حقبة نووية مظلمة للكوكب

لقد عبر العالم إلى حقبة نووية جديدة، حيث يكون الخطأ المشؤوم - وليس العدوان المتعمد - هو المحفز المحتمل للكارثة النووية. تم تحذير الزعماء الأمريكيين مرارًا من الصواريخ الروسية القادمة - في كل حالة، كان هذا إنذارًا خاطئًا نتج عن خطأ فني أو بشري. تم تنبيه الرئيس الروسي السابق بوريس يلتسين عن طريق الخطأ إلى ضربة صاروخية أمريكية محتملة بعد إطلاق صاروخ علمي نرويجي وسنفصل الحادثة تباعاً في هذا الفصل. بعد كل حادث، نخدع أنفسنا بأننا قادرون على حل المشكلة بتكنولوجيا أعقد وتدريب أفضل - أو نطمئن أنفسنا بأنّ مزيجًا من الاجتهاد والحظ السعيد كالذي شهدناه خلال فترة الحرب الباردة سيستمر. ولكن هل نعتقد حقًّا أنه يمكننا الحيلولة دون وقوع كارثة نووية إلى أجل غير مسمى في عالم يوجد فيه تسع دول تمتلك أسلحة نووية وشكوك كبيرة وعداء في العديد من علاقاتهما المتبادلة؟تتفاقم مخاطر الأخطاء البشرية التي تنطوي على الأسلحة النووية من خلال احتمال تهديدات الإنترنت المتعمدة (اختراق البيانات أو اختراق الخصوصية لأحد العاملين في أنظمة الإطلاق) لأنظمة الإنذار والقيادة والسيطرة. يمكن للقراصنة إدراج تحذير خاطئ من هجوم نووي في أنظمة الإنذار والإنذار الوطنية ويعزو هذا الهجوم كذباً إلى بلد بريء. في وقت يشهد توترات عالمية متصاعدة - مع القليل من التواصل أو التعاون بين الخصمين النوويين، ودقائق فقط من وقت اتخاذ القرار - كيف سيكون رد فعل قادة الدول الحائزة للأسلحة النووية؟مع إعلان إدارة دونالد ترامب مؤخرًا عن خطط لتوسيع دور الأسلحة النووية في الدفاعات الأمريكية بما يتجاوز ردع الهجمات النووية على الولايات المتحدة وحلفائها فإننا أمام تصاعد لفرص الاشتباك النووي في المستقبل القريب. حيث تنص استراتيجيتها الجديدة للأمن القومي على أن الترسانة الآن «ضرورية» ليس فقط لمنع شن هجوم نووي ولكن أيضًا «هجمات استراتيجية غير نووية، وعدوان تقليدي واسع النطاق.»



الصورة (12) شكل تخطيطي لمركز إطلاق الصواريخ النووية العابرة للقارات (السايلو) والذي يعتبر مركز تحكم عالي التعقيد وشديد التحصين لحمايته من أي ضربات نووية (معاكسة قوى) من قبل العدو، ويتكون من بناء عمودي متعدد الطبقات (حاضن الصاروخ) مرتبط بنفق أفقي بينه وبين مركز التحكم والسيطرة مع مهاجع الجنود ونقطة استخبارية.

إنّ توسيع نطاق التهديدات التي قد تستخدم ضدها الأسلحة النووية - مما يعني، على سبيل المثال، الهجمات الإلكترونية «الاستراتيجية» - سيزيد بشكل كبير من مخاطر سوء التقدير أو الخطأ. إذا كانت إحدى الهجمات الإلكترونية قد أخرجت جزءًا كبيرًا من شبكتنا الكهربائية، فهل سنكون قادرين على تحديد البلد المهاجم بسرعة وثقة؟إذا تبنت روسيا والصين والهند وباكستان وغيرها سياسات مماثلة، فهل نسير في طريق يصبح فيه الاستخدام النووي محتملاً إلى حد كبير؟

كل بلد يمتلك أسلحة نووية ينظر إلى ظروفه الجيوسياسية بشكل مختلف، لكننا جميعًا نواجه مخاطر نووية متزايدة. فرديًا عند الضرورة، ومعًا عند الإمكان، يجب عليهم التحرك بإلحاح بشأن السياسات التي يمكن أن تقلل من هذه المخاطر لجميع الدول، نوصي ثلاث خطوات أولية:

أولاً، يجب على الدول التي تمتلك أسلحة نووية أن تستعرض وتحمي بشكل مستمر من تعرض أنظمة الإنذار والقيادة النووية التهديدات السيبرانية. يجب أن يكون التركيز على تصحيح نقاط الضعف الحالية وإنشاء عملية تقييم وتحديث مستمر. يمكن مشاركة بعض النتائج والاستنتاجات مع القوى النووية الأخرى - مما يقلل المخاطر للجميع. يجب أن يدرك كلا منهما أن الهجوم الإلكتروني ضد أنظمة الإنذار والقيادة النووية هو وصفة لكارثة عالمية.

ثانياً، على الرغم من الخلافات الكبيرة حول العديد من القضايا العالمية، يجب على الولايات المتحدة وروسيا والدول المسلحة نوويًّا الأخرى العمل سويًا في مجالات ذات اهتمام مشترك وجودي - وأهمها الحد من خطر حدوث خطأ نووي. ما إن يتم إطلاق صاروخ باليستي نووي لسوء الحظ لا يمكن تذكره قبل أن يصل إلى هدفه. إن إزالة الأسلحة النووية الأمريكية والروسية من مواقف «الإطلاق الفوري» في حقبة الحرب الباردة - حيث تكون جاهزة للإطلاق وضرب أهدافها في غضون دقائق (21 دقيقة من أمر الإطلاق) - من شأنه أن يزيل «مسببات الشعر» ويزيد من وقت اتخاذ القرار للقادة. من خلال القيام بذلك، ستشكل واشنطن وموسكو مثالاً لجميع الدول التي تمتلك أسلحة نووية. يجب أن يكلف قادتهم الخبراء العسكريين في كل من هذه البلدان باستكشاف هذا الأمر وخيارات أخرى من شأنها أن تمنحهم مزيدًا من الوقت لاتخاذ قرارات مصيرية بشأن الاستخدام النووي.

ثالثًا، يتعين على الولايات المتحدة وروسيا تعزيز المبدأ - الذي تم التعبير عنه ببلاغة من قبل رونالد ريغان وميخائيل غورباتشوف - وهو أنه لا يمكن كسب حرب نووية ولا يجب خوضها أبدًا. هل نسيت أكبر قوتين نوويتين هذا الإنجاز التاريخي القوي الذي كان ضروريًا لإنهاء الحرب الباردة؟يجب أن تكون الأولوية الأكثر إلحاحًا هي هيكلة القوات النووية الأمريكية والروسية ووضعها لردع الاستخدام النووي وتقليل خطر الإطلاق غير المقصود أو الخطأ أو غير المصرح به (من جراء الهجمات السيبرانية خصوصاً واختراق أنظمة الإطلاق الصاروخية). في ظل هذه الخلفية، فإن المفهوم الروسي الحالي المتمثل في «التصعيد إلى التراجع» - أي الاستخدام النووي المحدود المصمم لإنشاء وقفة في الصراع وفتح طريق تسوية متفاوض عليها بشروط موسكو - وتدعو الولايات المتحدة إلى المزيد من الأسلحة النووية «القابلة للاستعمال» مجتمعة تجعل العالم مكاناً أكثر خطورة. يجب أن يكون لدى الولايات المتحدة أو أي دولة أخرى تمتلك أسلحة الدمار الشامل، رادع نووي آمن وموثوق طالما كانت الأسلحة النووية موجودة. لكن في العصر النووي

اليوم، لم يكن هذا كافياً. لا يزال هناك متسع من الوقت للعالم للالتقاء للحد من التهديدات النووية والقضاء عليها في نهاية المطاف - بشكل أكثر إلحاحًا من خلال اتخاذ إجراءات لتقليل مخاطر وقوع حادث أو خطأ أو سوء تقدير. يجب أن يكون هذا مبدأً أساسيًّا وهدفًا رئيسيًّا في تشكيل السياسة النووية لإدارة ترامب أو أي إدارة أمريكية أخرى.



صورة (13) مجموعة من الخبراء والعلماء وهم أمام ساعة يوم القيامة والتي تشير إلى الخطر المحدق بالبشرية من خلال الأزمات العالمية المحتدمة والكبرى التي تهدد كوكب الأرض بشكل عام ومنها الحروب الرقمية واحتمال اندلاع حرب نووية أو تفشي وباء عالمي قاتل أو تغيير كبير في المناخ (المصدر: فوكس نيوز 21 - حساب تويتر).

لا يزال هناك عشرات الآلاف من الأسلحة النووية الحرارية في الصوامع والغواصات، خاصة في الولايات المتحدة وروسيا، وكذلك في الصين وعدة دول أخرى. على الرغم من أن القوتين النوويتين الرئيسيتين وقعتا في عام 1994 اتفاقية لوقف استهداف مدينة ومنشآت بعضها البعض بصواريخ، إلا أنه يمكن اختيار الأهداف وإطلاق الأسلحة في غضون لحظة. من بين الرؤوس الحربية النووية السبعة والعشرين الموجودة حاليًا، تحتفظ الولايات المتحدة وروسيا بما مجموعه أكثر من خمسة آلاف رأس جاهزة للإطلاق في غضون دقائق قليلة بناءً على أوامر عُليا تصدر في حالة نشوب نزاع عالمي!

6.4حوادث على شفا حفرة الكارثة

لا يزال من الممكن حدوث عمليات إطلاق عرضية لصواريخ بالستية نووية عابرة للقارات، وحتى حرب نووية عارضة كاملة، حتى في هذه الأيام من السلام العالمي النسبي الهش. إن حادثة عام 1995، التي أبرزها خبراء الأمن مؤخرًا، توضح مدى السرعة التي قد يضع بها الإنذار الخاطئ العالم على شفا الحرب. في يناير من ذلك العام المليء بأحداث كبرى مثل (حرب الشيشان وأزمة الجيش الروسي المالية)، تم إطلاق صاروخ من ستة أطنان من ساحل النرويج، على بعد 300 ميل من الحدود الروسية، في مهمة علمية روتينية: لدراسة أورورا بورياليس (Aurora Borealis) (الأضواء الشمالية القطبية)، بول كيلي، أستاذ بجامعة كورنيل من صمم بعض المعدات، أفاد أنه وزملاءه كانوا حريصين على إخطار الروس بوقت الإطلاق والغرض منه ومساره، فقط في حالة وقوع حادث. لسوء الحظ، حدث خطأ كبير. هبت الرياح العاتية الصاروخ خارج المسار مباشرة نحو الأراضي الروسية.



صورة (14) سايلو صاروخ نووي جاهز للإطلاق وعلى أعلى درجات التأهب العمليات، في إحدى القواعد العسكرية الأمريكية. في حالة اختراق رقمي لأي شبكة مرتبطة بتلك القواعد أو العاملين فيها فإن مخاطر الإطلاق العرضي أو المتعمد سترتفع بشكل كبير

(المصدر: Brendan Smialowski/AFP/Getty Images).

لأسباب غير معروفة، لم يكن الروس يعرفون عن مهمة وتوقيت الإطلاق - لقد نسي أحدهم تسجيله وأخطأ في معطيات الصاروخ ترايدنت. تحتوي صواريخ ترايدنت على ثمانية رؤوس حربية نووية وتمثل واحدة من أسوأ مخاوف روسيا. فعلياً يمكن لصاروخ ترايدنت واحد إنْ تم إطلاقه على سان بطرسبرغ أن يدمر تلك المدينة عن بكرة أبيها. إن الصمامات القصيرة (short fuses) للقوات الاستراتيجية النووية الأمريكية والروسية زادت بشكل خاص من خطر نشوب حرب نووية عرضية، في حين أن «تطور التهديد السيبراني {للأسلحة النووية} زاد بشكل كبير» خلال العقد الماضي. هذا التهديد قد يكون له عواقب وأشكال مختلفة، بما في ذلك إيقاف تشغيلها (Shutting off weapons system)، أو إعطائها معلومات خاطئة (misinformation deployment)، أو في حالة بالغة الشدة، إطلاقها بطريق الخطأ (false launching initiatives). يتم الحفاظ على الترسانات الاستراتيجية بشكل مستمر في حالة تأهب قصوى. مئات

الصواريخ التي تحمل ما يقرب من 1800 رأس حربي جاهزة للطيران في غضون لحظة كما شرحنا في الأقسام السابقة من هذا الفصل. على شفا هذا الصراع، قد تُحاصر شبكات التسلل والقيادة النووية في جميع أنحاء العالم من قبل المتسللين الإلكترونيين الذين يتسبب هجومهم في تدهور تماسك وعقلانية صنع القرار النووي»

أولاً، يمكن للمهاجمين المتطورة قدراتهم العملياتية والتقنية من الفضاء الإلكتروني أن يخدعوا شبكات الإنذار المبكر الأمريكية أو الروسية في الإبلاغ عن إطلاق صواريخ نووية، الأمر الذي يتطلب ضربات انتقامية فورية وفقًا لمذاهب الحرب النووية لكلتا الدولتين.

ثانياً، يمكن للمتسللين عبر الإنترنت معالجة أنظمة الاتصالات لإصدار أوامر إطلاق غير مصرح بها لأطقم الصواريخ.

ثالثًا وأخيرًا، يمكن للمهاجمين اختراق أنظمة القيادة والسيطرة الصاروخية التي تطلق السلاح أو تفكيكه في الموقع (سيناريو غير مرجح للغاية)

لتقليل احتمالية حدوث مثل هذا السيناريو، اقترح أحد خبراء الاستراتيجيات المختصة بسياسات الدفاع والاستخبارات (اللواء الأمريكي المتقاعد جيمس كارترايت) أن تقوم موسكو وواشنطن بتعديل الجداول الزمنية لخطة الطوارئ الخاصة بالحرب النووية من الدعوة إلى إطلاق الصواريخ في غضون ثلاث إلى خمس دقائق إلى 24 إلى 72 ساعة. حيث أكد هذا الخبير من خلال نقاشات طويلة مستفيضة أن تخفيض مهلة إعداد الصواريخ النووية لإطلاقها لن يقلل من قيمة الردع للأسلحة، كما أكد كارترايت، الذي ترأس القيادة الاستراتيجية من 2004 إلى 2007 وكان نائب رئيس هيئة الأركان المشتركة قبل التقاعد في 2011. ومع ذلك، رفض البيت الأبيض في معظم الإدارات تلك الفكرة حتى الآن، لا سيما بسبب التدهور الأخير في العلاقات الأمريكية الروسية. حيث كان التعليل العسكري هو «لم يكن من المنطقي إزالة القوات من حالة التأهب» لأن الصواريخ النووية «يجب أن تكون جاهزة وفعالة وقادرة على مقاضاة العدو صاحب الهجوم في أي وقت. في نهاية المطاف لقد أوصلتنا الأسلحة والاستراتيجيات السيبرانية إلى حالة من عدم الاستقرار النووي المتفاقم والتي تحتاج إلى معالجة أكثر صراحةً وانفتاحاً في دبلوماسية القوى الكبرى، في القطاعين العام والخاص. لا يهدف القلق هنا إلى التقليل من الآثار المدمرة والفورية للهجوم النووي. ولكن بدلاً من ذلك، يجب الإشارة إلى أن بعض وسائل الحماية الدولية ضد النزاعات النووية تكاد تكون

معدومة ضد الهجمات السيبرانية المتنامية في السنوات الأخيرة والأمثلة كثيرة ومتنوعة حول حوادث مميتة وكارثية حدثت ولم تؤخذ بالحسبان. على سبيل المثال، تشير فكرة «التدمير المتبادل المؤكد» إلى أنه لا ينبغي لأي دولة إطلاق سلاح نووي على دولة أخرى مسلحة نوويًا، فمن المحتمل أن يتم الكشف عن الإطلاق، وأن الدولة المستهدفة ستطلق أسلحتها الخاصة ردّاً على ذلك، وتدمير كلا البلدين. المهاجمون السيبرانية لديهم عدد أقل من الموانع؛ لسبب واحد، من السهل إخفاء مصدر التوغل الرقمي أكثر من إخفاء المكان الذي ينطلق منه صاروخ. علاوة على ذلك، يمكن أن تبدأ الحرب الإلكترونية صغيرة، وتستهدف حتى هاتفًا واحدًا أو كمبيوتر محمولًا واحدًا. قد تستهدف الهجمات الأكبر الشركات، مثل البنوك أو الفنادق، أو وكالة حكومية. لكن هؤلاء ليسوا كافيين لتصعيد النزاع إلى المستوى النووي.

6.5 الهجمات السيبرانية النووية

هناك ثلاثة سيناريوهات أساسية لكيفية تطور الهجوم السيبراني النووي. يمكن أن تبدأ بشكل متواضع، مع قيام جهاز مخابرات دولة ما بسرقة أو حذف أو المساس بالبيانات العسكرية لدولة أخرى. جولات متتالية من الانتقام يمكن أن توسع نطاق الهجمات وشدة الأضرار التي لحقت بالمدنيين. في حالة أخرى، يمكن لدولة أو منظمة إرهابية أن تطلق هجومًا إلكترونيا مدمرًا على نطاق واسع - يستهدف العديد من مرافق الكهرباء أو منشآت معالجة المياه أو المنشآت الصناعية في وقت واحد، أو بالاشتراك مع بعضها البعض لتفاقم الضرر. ربما يكون أكثر ما يثير القلق هو أنه قد يحدث عن طريق الخطأ. في عدة مناسبات، دمرت الأخطاء البشرية والميكانيكية العالم خلال الحرب الباردة؛ يمكن أن يحدث شيء مشابه في البرامج والأجهزة في المجال الرقمي. مثلما لا توجد وسيلة للحماية الكاملة ضد أي هجوم نووي، هناك طرق فقط لجعل الهجمات الإلكترونية المدمرة أقل احتمالًا: الأول هو: أن الحكومات والشركات والأفراد العاديين بحاجة إلى تأمين أنظمتها لمنع المتسللين الخارجيين من الوصول إلى طريقهم، ثم استغلال اتصالاتهم والوصول أو الغوص بشكل أعمق داخل تلك الشبكات. الأنظمة الحرجة، مثل تلك الموجودة في المرافق العامة وشركات النقل والشركات التي تستخدم المواد الكيميائية الخطرة، تحتاج إلى أن تكون أكثر أمانًا. وجد أحد التحليلات الاستخبارية أن حوالي خمس الشركات التي تستخدم أجهزة الكمبيوتر للتحكم في الآلات الصناعية (industrial automation systems) في الولايات المتحدة فقط تقوم بمراقبة أجهزتها للكشف عن الهجمات المحتملة - وأنه في 40 في

المائة من الهجمات التي قاموا بصيدها، كان الدخيل يصل إلى النظام من أكثر من سنة. ووجد مسح آخر أنّ ما يقرب من ثلاثة أرباع شركات الطاقة (خاصة في المحطات الكهرونووية) قد شهدت نوعًا من التسلل إلى الشبكة في العام السابق. ولكن لا يمكن حماية جميع هذه الأنظمة دون وجود موظفين مهرة في مجال الأمن السيبراني للتعامل مع العمل الخطر في تلك الحالات. في الوقت الحاضر، ما يقرب من ربع جميع وظائف الأمن السيبراني في الولايات المتحدة شاغرة، مع وجود عدد من المناصب التي يتم فتحها أكثر من الأشخاص الذين يشغلونها. حيث أعرب أحد خبراء الموارد البشرية في المحطات النووية عن قلقه من أن بعض الوظائف التي يتم شغلها يشغلها أشخاص غير مؤهلين للقيام بها. الحل هو مزيد من التدريب والتعليم، لتعليم الناس المهارات التي يحتاجون إليها للقيام بالأمن السيبراني، والاطلاع المستمر للعاملين الحاليين على أحدث استراتيجيات التهديدات والدفاع.



الصورة (15) منظر عام لكابينة (نموذج قديم) مركز التحكم المركزية بإحدى سايلوات الصواريخ النووية العابرة للقارات وفيها تظهر الأجهزة التماثلية التي مازالت فعالة إلى اليوم ولم يتم تحديثها إلا مؤخراً مما يجعلها عرضة للاختراقات السيبرانية وسرقة البيانات أو التلاعب بها.

إذا كان على العالم أن يوقف الهجمات السيبرانية الكبرى - بما في ذلك بعضها مع احتمال أن يكون ضررًا مثل الضربة النووية - فسيكون الأمر متروكًا لكل شخص ولكل شركة وكل وكالة حكومية للعمل من تلقاء نفسها ومعًا لتأمين الأنظمة الحيوية التي تعتمد على حياة الناس. إننا أمام تحديات هائلة في مجال الأمن السيبراني الصناعي والنووي! خاصة في هذا الزمن الصعب والمعقد، خلال وقت السلم، ستخلق الأنشطة السيبرانية الهجومية معضلة للدولة ومؤسساتها لأنها قد لا تعرف ما إذا كانت أنظمتها الحيوية ومنها النووية قد تعرضت لهجمات إلكترونية - سيبرانية! في حين أن التركيز الرئيسي للتحدي السيبراني في «العصر السيبراني» المزدهر يميل إلى التركيز على القرصنة أو البرمجيات الخبيثة أو القنابل المنطقية أو هجمات الحرمان من الخدمة، فربما يكون التحدي الأدق هو التحدي الذي لا علاقة له بهجمات أو أسلحة على الإطلاق. في الواقع، واحدة من أكبر التحديات هي المشاكل الطبيعية والكوارث و«الأخطاء» الموجودة في برامج الترميز المعقدة والمتقدمة المستخدمة بشكل كبير في برامج الأسلحة النووية. بشكل عام، من المحتمل أن تحتوي على المزيد من الأخطاء والمشكلات الفنية البرمجية والأخطاء غير المتوقعة، خاصة تلك التي تعتمد

على تعليمات برمجية - لوغاريتمية معقدة، وتربط بين وظائف وأجهزة متعددة، ويجب عليها إجراء حسابات دقيقة بسرعة متناهية، وهنا تكمن الكارثة. إذًا هناك أربعة مجالات أساسية يمكن أن تؤثر فيها الأسلحة السيبرانية على استقرار الأزمات بين الجهات الفاعلة المسلحة نووياً:

(1) يمكن أن تؤدي إلى تعطيل أو تدمير قنوات الاتصال، مما يجعل من الصعب إدارة القوات أثناء النزاع وتقليل ثقة القادة في أنظمتهم؛ لأن «يجب أن يكون عدد قليل فقط من الهجمات ناجحًا في زرع بذور الشك في أي معلومات قادمة من جهاز كمبيوتر» - أو قد تشمل هجمات حجب الخدمة الموزعة (DDoS).

(2) يمكن أن تزيد من الضغوط الزمنية المتصورة للعمل / الاستجابة أو التصرف الوقائي.

(3) قد تقلل من البحث عن بدائل تقنية قابلة للتطبيق في وقت قصير (أزمة الزمن الفعلي للاستجابة)،

و(4) قد تتسبب في ظهور صور معيبة للنوايا والقدرات العسكرية، مما يؤدي إلى تفاقم مخاوف «المفاجأة الاستراتيجية، وخلق مشاكل كبيرة للإشارة الناجحة للردع أو التفاوض الندي». وبهذه العوامل مجتمعة، تثير تلك الديناميكا السيبرانية ذات الطبيعة الاختراقية التدميرية أو حتى الناعمة، احتمال تصعيد (غير مقصود) وربما لا يمكن السيطرة عليه وتجعل إدارة مثل هذه الأزمات أكثر تعقيدًا وخطورة. في هذه الحالة، قد تصل الولايات المتحدة وروسيا أو الهند وباكستان أو الهند والصين إلى حافة الحرب النووية.

الفصل السابع
نبوءة أورويل

7.1 أسطورة الأمن

«من يتحكم بالماضي يتحكم بالمستقبل.
ومن يتحكم بالحاضر يتحكم بالماضي»

جورج أورويل (1950)

استعرنا هذا العنوان من الكاتب الهولندي المتميز «بارت ده كونج»، تخصص هذا الكاتب في مسألة الأمن والأمان في أوروبا وخاصة في بلده هولندا وكتب في هذا الموضوع العديد من الكتب (منها الكتب التالية: التنظيم في مسألة الأمن، أسطورة الأمن، كل شيء تحت السيطرة). ينتقد الكاتب استسلام المجتمع الأوروبي لسيل الأخبار الخاصة بالأمن ومن قبول كافة الإجراءات الأمنية الناجمة عن هذه الأخبار، فالنهاية القرن الماضي حسب رأيه شهدت صعودًا مذهلًا لفكرة الأمن والأمان أكثر من أي فترة سابقة وبدأ المواطن الأوروبي قبل غيره يصبح حبيسَ مصطلحاتِ الأمن وبدأ يطالب به، يؤكد «ده كونج» بعد دراسته المعمقة للحالة الأوروبية وجود فجوة بين المواطن والدولة: «المواطن بات يشكك بالدولة ومؤسساتها وسياسيها وعلمائها وقضاتها وسلطة القانون فيها». لكنه في الوقت ذاته يطالبها بتوفير نسبة 100% من الأمان. وتعده الحكومات في كل انتخابات بالمقابل بالنسبة ذاتها من الأمان وإزالة مشاعر القلق؛ لأجل ذلك تتوجه الحكومات دون قلق لاتخاذ مزيد من الإجراءات لتحقيق ذلك. المواطن يقبل بها ويطلب المزيد لتحقيق الأمان والأمن الموعود. لعله حتى هذه اللحظة لم يدرك بعد أنه قدّم الكثير من أجل الحصول على الأمان المنشود. في هذا العالم المظلم، لا وجود لمصطلح الخصوصية إطلاقاً. تعرف شركات التكنولوجيا الفائقة

والمعلومات كل ما يمكن معرفته عن الأشخاص، بدءًا من الموانع الأعمق من خلال تفضيلاتهم الجنسية إلى أنواع الزبادي المفضلة لديهم من الفراولة. تستطيع الخوارزميات المتطورة، من النوع الذي جعل شخص مثل Mercer أنجح متداول إلكتروني في العالم، الذي قام بتحليل وتصنيف تريليونات من تيرابايت من المعلومات الشخصية ومن ثم التنبؤ بدقة 99.9% بكيفية تفاعل الناس مع أي موقف أو شعار معين. على سبيل المثال، يجلس عدد قليل من مديري الحلقات النقاشية - ميرسر وبانون - في غرفة عمليات معزولة ويقررون الاستراتيجية العامة لحملة الانتخابات الرئاسية الأمريكية، ثم ينشئ العلماء والحواسيب والخوارزميات والذكاء الاصطناعي في الواقع الافتراضي الذي سوف يغلف الناخبين وكذلك الرسائل والشعارات التي تثير غضبهم بما يكفي لضمان أدلائهم بأصواتهم للرجل المرسَل إليه للقيام بهذه المهمة؛ في هذه الحالة، بعد عسر الولادة الطويل، كان هو الرئيس دونالد ترامب.

إنّ قصة السيرة الذاتية لرواية العام 1984 - كانت سباق الرجل المحتضر مع الزمن لإنهاء روايته في كوخ بعيد في جزيرة جورا، قبالة ساحل اسكتلندا - ستكون مألوفة لدى العديد من قراء أورويل. تتمثل إحدى مساهمات Lynskey في تدمير الفكرة القائلة إن رؤيتها المرعبة يمكن أن تُعزى إلى الرغبة في وفاة مريض السل، أو تجاهله بطريقة ما. في الواقع، أثار المرض الحاد في أورويل غضبًا للعيش - وتزوج مرة أخرى على فراش الموت - تمامًا كما يتم تخفيف تشاؤم الرواية، حتى صفحاتها الأخيرة، من خلال ارتباط وينستون سميث بالطبيعة، والأشياء العتيقة، ورائحة القهوة، والصوت من الغناء البروليتاري، وقبل كل شيء حبيبته، جوليا. 1984 قاتمة للغاية، لكن وضوحها وصرامتها منبهات للوعي والمقاومة الاجتماعية والشعبية. وفقا ل- (لينسكي)، «لا شيء في حياة أورويل وعمله يدعم تشخيص اليأس.» تتبع لينسكي التكوين الأدبي للعام 1984 إلى القصص الخيالية للقرن التاسع عشر المتفائل - إدوارد بيلامي في نظرة إلى الوراء (1888)؛ روايات الخيال العلمي لـ H. G. Wells، التي قرأها أورويل كصبي - وخلفائهم الدستوريين في القرن العشرين، بما في ذلك الروائي الروسي Yevgeny Zamyatin’s «We» (1924) و(Huxley’s «Brave New World World» (1932. إنّ الصفحات الأكثر إثارة للاهتمام في «وزارة الحقيقة» هي سرد لينسكي للحياة الآخرة (Afterlife) للرواية. بدأ الصراع على الادّعاء بأن رواية «1984» فور نشرها، مع معركة حول معناها السياسي. خلص المراجعون الأمريكيون المحافظون إلى أن الهدف الرئيسي لأورويل لم يكن فقط الاتحاد السوفيتي ولكن اليسار عمومًا.

تلاشى أورويل سريعًا مع بيان يوضح أن الرواية لم تكن هجومًا على أي حكومة بعينها بل هجاء للاتجاهات الشمولية في المجتمع الغربي والمثقفين: «الأخلاقية التي يمكن استخلاصها من هذا الوضع الخطير من الكابوس هي حالة بسيطة: لا تدع ذلك يحدث. هذا يعتمد عليك «. لكن كل عمل فني يهرب من سيطرة الفنان - وكلما زادت شعبية وتعقيد، زاد سوء التفاهم. إنّ رواية لينسكي عن مدى أهمية سردية عام 1984 هو كشف لعمقها الاجتماعي والفني. ألهمت الرواية الأفلام والبرامج التلفزيونية والمسرحيات والباليه والأوبرا حتى ألبوم ديفيد باوي الشهير استمد بعض قفشاته منه والتقليد والمحاكاة الساخرة والتكميلية والرفض، لي هارفي أوزوالد، وحزب النمر الأسود، وجمعية جون بيرش. لقد اكتسبت شيئًا من الوجود الخانق لـ Big Brother نفسه: 1984 يراقبك هذه كانت كل الإشارات والاقتباسات الاجتماعية. مع وصول عام 1984، ارتفعت الاعتمادات الثقافية لتلك الرواية إلى مستوى يصم الآذان، لقد انتشرت في كل مكان تقريباً على سطح الكوكب.

تتكرر الحجة الخاصة بالرواية كل عشر سنوات أو نحو ذلك: لقد أخطأ أورويل أليس كذلك. الأمور لم تكن بهذا السوء، بكل تأكيد أن الاتحاد السوفيتي أصبح من التاريخ. التكنولوجيا تتحرر وتصبح منصات للتعبير الحر. لكن أورويل لم يقصد قط أن تكون روايته بمثابة تنبؤ للأحداث، بل مجرد تحذير. وهذا تحذير هو أن عام 1984 مستمر في العثور على أهمية جديدة في المجتمعات. في خلال الأسبوع الذي تم فيه تنصيب الرئيس دونالد ترامب رئيساً للولايات المتحدة، عندما برر مستشار الرئيس كيليان كونواي تقديره الزائف للحشود باستخدام عبارة «حقائق بديلة» Alternative facts، عادت الرواية إلى قوائم أكثر الكتب مبيعًا. وجلب انتخاب ترامب مجموعة من الكتب التحذيرية بعناوين مثل On Tyranny، وFascism: A Warning، وكيف تعمل الفاشية إلى الواجهة من جديد. أقامت مكتبة بيع الكتب المحلية طاولة ذات طابع استبدادي ووضعت الكتب الجديدة بجانب عام 1984. وأشاروا إلى القرن العشرين - إذا حدث ذلك في ألمانيا، فقد يحدث ذلك هنا - وحذروا القراء من انهيار الديمقراطيات بسهولة. لقد كانوا أجراس إنذار ضد الرضا والقدرية - «سياسات الحتمية»، على حد تعبير المؤرخ تيموثي سنايدر، «شعور بأن المستقبل أكثر حاضرًا، أن قوانين التقدم معروفة، أنه لا يوجد لقد كانت التحذيرات مبررة، لكن تركيزها على آليات الديكتاتوريات السابقة لفت الانتباه بعيدًا عن قلب الورم الخبيث - وليس الدولة، بل الفرد. لم تكن القضية الحاسمة هي أن ترامب قد يلغي الديمقراطية المعروفة بشكلها الحالي، بل أن الناخبين الأمريكيين وضعوه في وضع يسمح له

بالمحاولة تلك. أن ذلك التخويل غير المحترم اليوم هو طوعي إنه يأتي من الأسفل (القاعدة الشعبية) إلى الأعلى (القيادة العليا للبلد) وصناع القرار.

نحن نعيش مع نوع جديد من النظام لم يكن موجودًا في زمن أورويل. فهو يجمع بين القومية الصعبة - حيث يتم تحويل الإحباط المزمن والسخرية إلى كره الأجانب والكراهية للآخر المختلف - مع الارتباك اللين ليصبح مزيجًا من أورويل وهكسلي فيه القسوة والترفيه الممتزج بنوع من الدراما السوداوية. الحالة الذهنية التي يفرضها الحزب «الحاكم» من خلال الإرهاب الفكري في رواية عام 1984، حيث تصبح الحقيقة غير مستقرة وباهتة لدرجة أنه لم يعد لها وجود (تماماً كما نرى في الشبكات الاجتماعية ومواقع الإنترنت التي تنشر أخبار مزيفة. تعمل الدعاية الشمولية على توحيد السيطرة على جميع المعلومات، حتى يصبح الواقع هو ما يقوله الحزب فقط - هدف Newspeak هو إفقار اللغة بحيث لم تعد الأفكار غير الصحيحة سياسياً ممكنة. المشكلة اليوم هي أن الكثير من المعلومات من العديد من المصادر أغلبها يحمل رسالة مشوشة وضبابية حول الحقائق، مع الطاعون الناجم عن التفتت والانقسام المجتمعي - وليس فقط السلطة المفرطة حيث أدت إلى اختفاء الثقة بشكل كلي لدى الجمهور، الأمر الذي يترك الناس العاديين للعمل على اكتشاف الحقائق بأنفسهم، تحت رحمة التحيز والأوهام الخاصة بهم.

7.2 حملة 2016 الرئاسية وقصة خرافة الخصوصية الشخصية

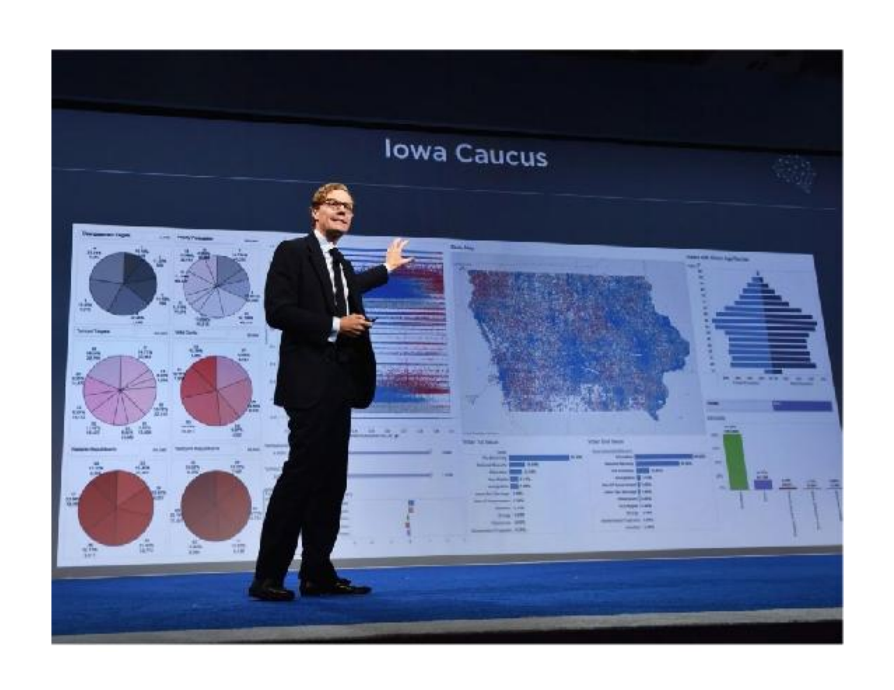
خلال الحملة الرئاسية الأمريكية لعام 2016، استخدم دعاة الدعاية في مزرعة روسية للتجول وسائل التواصل الاجتماعي لنشر مذكرة: «الشعب يصدق ما يقوله الإعلام لهم -« جورج أورويل. «لكن أورويل لم يقل هذا أبدًا. سُرقت السلطة الأخلاقية لاسمه وتحولت إلى كذبة تجاه تلك الغاية الأورويلية: تدمير الإيمان بالحقيقة. احتاج الروس إلى شركاء في هذا الجهد ووجدهم الملايين، وخاصة بين غير النخب الأمريكية. في عام 1984، يُطلق على الناس من الطبقة العاملة اسم «proles»، ويعتقد Winston أنهم الأمل الوحيد للمستقبل. كما يشير لينسكي، لم يتنبأ أورويل بأن الرجل والمرأة العاديين يستقبلان التفكير المزدوج بحماس مثل المثقفين، وبدون الحاجة إلى الإرهاب أو التعذيب، سيختارون الاعتقاد بأن ناتج اثنين زائد اثنين كان كل ما يريدونه. يتم فرض الأرثوذكسية (التفكير المتعنت أو المتصلب) أيضًا عن طريق الضغط الاجتماعي، وليس في أي مكان تظهر تلك العملية واضحة أكثر من موقع Twitter، حيث ينتج شبح الخجل أو «الإلغاء»

المطابقة بقدر ما يحدث احتمال الإضافة إلى قبيلتك من أتباعك. يمكن أن يكون هذا الضغط أقوى من حزب أو دولة، لأنه يتحدث باسم الشعب ولغة الغضب الأخلاقي، الذي لا يوجد ضده أي دفاع. يقوم بعض المفوضين (أصحاب الحسابات المتضخمة) ذوي الأتباع الكبيرة بدوريات في مواقع التواصل الاجتماعي ومعاقبة مجرمي الفكر (المخالفين في الرأي)، لكن معظم التقدميين يوافقون دون صعوبة على الإجماع الخانق للحظة والتعصب الذي يولده ذلك الإجبار الأحادي لتبني فكر ما - ليس بسبب الخوف، ولكن لأنهم وببساطة يريدون أن يتم احتسابه على الجانب ذي الأغلبية العادلة (القطيع الايجابي).

عندما يكرر ترامب القصة المضحكة عن ثلاثة ملايين ناخب غير شرعي - وهي قصة لا يعرفها أحد، وليس حتى «موظف صغير» بالبيت الأبيض، ولا أي عضو جمهوري واحد يعتقد فعلاً أنه تصريح يعتمد الحقيقة أو المهنية، فهو (اي ترامب) لا يهتم حقًا إذا كان هناك من يعتقد، حتى لو، على مستوى مجنون، أن يعتقد بصحة وجود هذا العدد الهائل من الناخبين الوهميين وأين، في الولايات المتحدة الأمريكية حيث يتم تسجيل كل شاردة وواردة لأكثر من 300 مليون نسمة وعلى مدار السنة. لا يقصد الناس تصديق ذلك النوع من الأكاذيب؛ ولكن من المفترض أن يتم تخويفهم بها. الكذبة ليست حول ادعاء حقائق محددة؛ بل الجنون هو تحد متعمد لفكرة التعقل الكبيرة بأكملها. بمجرد أن تكون الكذبة كبيرة في التداول العام والشعبي، تصبح محاولة إعادة المحادثة إلى منطقة الحجة المنطقية أمرًا مستحيلًا. في 27 أكتوبر 2012، كتب مارك زوكربيرج الرئيس التنفيذي لشركة Facebook رسالة بالبريد الإلكتروني إلى مدير تطوير المنتجات في ذلك الوقت. على مدار سنوات، سمح Facebook لتطبيقات الجهات الخارجية بالوصول إلى البيانات الخاصة بأصدقاء المستخدمين غير المرغوب فيها، وكان زوكربيرج يفكر فيما إذا كان التخلي عن كل هذه المعلومات ينطوي على مخاطرة. في رسالته الإلكترونية، أشار إلى أنه لم يكن: «أنا متشكك بشكل عام في أن هناك قدرًا كبيرًا من المخاطر الاستراتيجية لتسرب البيانات كما تعتقد»، كتب في ذلك الوقت. «لا يمكنني التفكير في أي حالات تسربت فيها هذه البيانات من مطور إلى مطور وتسببت في مشكلة حقيقية بالنسبة لنا.» إذا كان لدى زوكربيرج آلة زمنية، فقد يستخدمها للعودة إلى تلك اللحظة المروعة. من يدري ما الذي كان سيحدث لو أن الرئيس التنفيذي الشاب، في عام 2012، كان ليتصور كيف يمكن أن يحدث كل هذا الخطأ؟على الأقل، ربما كان قد أنقذ Facebook من السنة المدمرة التي مر بها بعد ذلك. لكن زوكربيرج لم يستطع رؤية ما هو الصحيح أمامه - ولا يمكن

لبقية العالم أن يرى ذلك فعلاً - حتى 17 مارس 2018، عندما أخبر أحد المبلغين (whistleblower) ذو الشعر الوردي كريستوفر ويلي صحيفة نيويورك تايمز وصحيفة الغارديان / أوبزرفر عن شركة تدعى Cambridge Analytica سيكون تردد اسمها في الأخبار والترندات العالمية اثراً كبيراً! من هي Cambridge Analytica؟هذه الشركة هي شركة استشارية وتحليلات للبيانات تم تمويلها من قبل الملياردير الأمريكي اليميني روبرت ميرسر وترأسها ستيف بانون مؤسس Breitbart قبل مغادرته للعمل كرئيس تنفيذي لحملة ترامب 2016. غطت التقارير كيفية استخدام Cambridge Analytica للبيانات لاستهداف الناخبين الفرديين واستهدافهم بهدف التنبؤ بقراراتهم الانتخابية والتأثير عليها. قامت شركة Analytica Cambridge بشراء بيانات فيسبوك لعشرات الملايين من الأمريكيين دون علمهم لبناء «أداة حرب نفسية»، والتي أطلقتها على الناخبين الأمريكيين للمساعدة في انتخاب دونالد ترامب رئيسًا. قبيل انتشار الأخبار، قام Facebook بحظر Wylie وCambridge Analytica، الشركة الأم SCL، وألكسندر كوغان، الباحث الذي جمع تلك البيانات الرقمية من المنصة (الفيس بوك). لكن تلك التحركات جاءت بعد فوات الأوان ولم تستطع كبح جماح غضب المستخدمين والمشرعين والمدافعين عن الخصوصية والمثقفين والإعلاميين. على الفور، انخفض سعر سهم Facebook وبدأت المقاطعة. تم استدعاء زوكربيرج للإدلاء بشهادته أمام الكونغرس، وبدأ عام من المناقشات الدولية المثيرة للجدل حول حقوق الخصوصية للمستهلكين عبر الإنترنت. يوم الجمعة، رفعت كوجان دعوى تشهير ضد Facebook. كان الاختلاف عندما روى ويلي هذه القصة في عام 2018، عرف الناس كيف انتهت - بانتخاب دونالد جيه ترامب. هذا لا يعني أن رد الفعل العنيف كان، كما ادعى ألكساندر نيكس الرئيس التنفيذي السابق لجامعة كامبريدج التحليلية، مؤامرة سيئة النية من جانب مناهضي ترامب غير راضية عن نتيجة الانتخابات. هناك أكثر من دليل كاف على ممارسات الشركة غير المجدية في الأعمال التجارية لضمان كل التدقيق الذي تلقته. ولكن من الصحيح أيضًا أن السياسة يمكن أن تزعزع الاستقرار، مثل نقل النتروجليسرين. على الرغم من النظريات والافتراضات التي كانت تدور حول كيفية إساءة استخدام البيانات، بالنسبة لكثير من الناس، فقد تطلب الأمر انتخاب ترامب، وعلاقات كامبريدج أناليتيكا الفضفاضة بها، ودور فيسبوك في ذلك لمعرفة أن هذا الشيء إسفنجي وغير ملموس يسمى الخصوصية له عواقب في العالم الحقيقي.

قد تكون Cambridge Analytica هي طفل الملصق المثالي (ideal marketing baby) لكيفية إساءة استخدام البيانات. لكن فضيحة كامبريدج التحليلية، كما كانت تسمى، لم تكن أبدًا عن الشركة وعملها. في الواقع، أصرت حملة ترامب مرارًا وتكرارًا على أنها لم تستخدم معلومات Cambridge Analytica، بل علماء البيانات فقط. ويشك بعض الأكاديميين والممارسين السياسيين في أن التنميط الشخصي ليس أكثر من زيت الثعابين. بدلاً من ذلك، نمت الفضيحة وزادت واتسعت ردود الفعل لتشمل الطرق التي تأخذ بها تلك الشركات، بما في ذلك على سبيل المثال لا الحصر Facebook، حيث هناك المزيد من بيانات الناس فائضة عما يحتاجون إليه، ويمكن أن تتخلى عنها بسهولة أكثر مما ينبغي، وغالبًا ما تطلب إذنًا فقط في الطباعة الدقيقة - إذا كانت حتى تنتبه لذلك على الإطلاق. أي أن تلك البيانات الشخصية قد تخليت عنها بإرادتك عندما وافقت على قواعد وقوانين الاستخدام.



الشكل رقم (16) ألكساندر نيكس وغيره من المسؤولين التنفيذيين السابقين في Analytica Cambridge تم استدعاؤهم إلى الكونغرس الأمريكي لمناقشة دور الشركة خلال انتخابات عام 2016

مرت أكثر من سنة واحدة منذ أن أصبحت أخباراً على الصفحة الأولى، حيث لا يزال مديرو كامبريدج Analytica مدعوين إلى الكونغرس للرد على تصرفاتهم المخزية خلال انتخابات 2016. ومع ذلك، فإن الحديث عن الخصوصية انتقل إلى حد كبير من الشركة التي انتهت صلاحيتها الآن، والتي أغلقت مكاتبها في مايو الماضي. هذا أمر جيد إذا كنا نفكر به من تلك الزاوية (وهي إيقاف أي شركة تنتهك خصوصياتنا). مع تلاشي Cambridge Analytica إلى الخلفية وانتهاء دورها التجاري والعمليات، برزت أسئلة مهمة أخرى، مثل كيفية قيام Facebook بتقديم صفقات بيانات خاصة إلى صانعي الأجهزة، أو لماذا تتعقب شركة Google موقع الأشخاص حتى بعد إيقاف خاصية تشغيل تتبع الموقع. كان هناك اعتراف متزايد بأنه لم يعد من الممكن ترك تلك الشركات لتنظيم نفسها في مسألة جمع البيانات الشخصية، وبدأت بعض الدول في العمل على ذلك. نفذت ولاية فيرمونت قانونًا جديدًا يلزم وسطاء البيانات الذين يقومون بشراء وبيع البيانات من أطراف ثالثة للتسجيل لدى الدولة وبشكل قانوني. في كاليفورنيا، من المقرر أن يصبح القانون ساري المفعول في كانون الثاني (يناير) من شأنه، من بين أمور أخرى، أن يمنح السكان القدرة على

الانسحاب من بيع بياناتهم. أدخلت عدة ولايات مشاريع قوانين مماثلة في الأشهر القليلة الماضية وحدها. في الكابيتول هيل، يدرس الكونغرس حدود قانون حماية البيانات الفيدرالي - رغم أن التقدم، كما هو الحال دائمًا في واشنطن، يسير بخطى بطيئة.



الصورة (16) الرئيس التنفيذي لعملاق شبكات التواصل الاجتماعي (الفيس بوك) وشركاتها الأخرى وهو يخضع لاستجواب الكونغرس في خصوص فضيحة شركة كامبريدج أناليتيكا والتي ساهمت في انتخاب ترامب سنة 2016 في الولايات المتحدة الأمريكية.

هذه الفضائح وردود الفعل أضرت الفيس بوك بشدة ويمكن القول إن صناعة التكنولوجيا بأكملها قد أصابتها كدمات لن تنسى. إذ واجه زوكربيرج مشكلة في تشخيص ورؤية «الخطر» المرتبط بحماية الخصوصية البطيئة في عام 2012، وبعد كل تلك المصائب فيجب عليه أن يكون على دراية بخطورته الآن. يواجه Facebook غرامة قياسية محتملة من قبل لجنة التجارة الفيدرالية، وقد كشفت الأخبار المتتالية أن الشركة تخضع لتحقيق جنائي بسبب سياساتها الخاصة بمشاركة البيانات الشخصية للمستخدمين. في الوقت نفسه، دفعت الآثار المترتبة على فضيحة كامبريدج أناليتيكا لفيس بوك إلى تغيير - على الأقل في بعض النواحي - من طرقها التقليدية في التعاطي مع خصوصية المستخدمين. في الأسبوع الماضي، في مدونة تدور حولها منافسة شديدة، ادعى زوكربيرج أن مستقبل Facebook يعتمد على الخصوصية. وقال إن Facebook سيضيف تشفيرًا شاملاً لكل من Messenger Facebook وInstagram Direct كجزء من خطة كبرى لإنشاء شبكة اجتماعية جديدة للاتصالات الخاصة. إن ما قامت به Cambridge

Analytica في قصة انتخابات الرئاسة الأمريكية هو نفسه ما كنا نراه في رواية 1984 وما كان النظام الأوتوقراطي يخطط له للاستحواذ الكامل على وعي وقرار الشعب من خلال التلاعب بالرسائل التي يريد تمريرها كخيار المواطنين المغلوب على أمرهم الذين سرقت منهم ارادتهم الحرة ليتم استبدالها بدمية مستنسخة منهم تم تشكيلها من قبل تلك الحكومات. وحيث سعى أورويل لإيقاظ المجتمعات البريطانية والأمريكية على الأخطار الاستبدادية التي هددت الديمقراطية حتى بعد الهزيمة النازية. في رسائل قبل وبعد الانتهاء من روايته، حث أورويل على «النقد المستمر»، محذرا من أن أي «حصانة» للاستبداد يجب ألّا يعتبر أمرًا مفروغًا منه: «الشمولية، إن لم تقاتل، يمكن أن تنتصر في أي مكان.» نجد أن أحداث الانتخابات الأمريكية أيقظت هذا الشعور المخيف لدى الكثير من الشرائح الشعبية. لمدة 19 عامًا، قامت الشركات الخاصة التي تمارس منطقًا اقتصاديًا غير مسبوق يمكن أن نسميه رأسمالية المراقبة باختطاف الإنترنت وتقنياته الرقمية بشكل ممنهج وواسع. تم اختراع هذا الاقتصاد الجديد في Google بداية من عام 2000، ويدعي سراً أن التجربة البشرية الخاصة هي مادة خام مجانية للترجمة إلى بيانات سلوكية. يتم استخدام بعض البيانات لتحسين الخدمات، ولكن يتم تحويل الباقي إلى منتجات حسابية تتنبأ بسلوكك. يتم تداول هذه التوقعات في سوق العقود الآجلة الجديد، حيث يبيع أصحاب رأس المال الرقابي اليقين للشركات المصممة على معرفة ما سنفعله بعد ذلك. تم تطبيق هذا المنطق لأول مرة على العثور على الإعلانات على الإنترنت التي ستجذب اهتمامنا، ولكن توجد ممارسات مماثلة الآن في كل قطاع تقريبًا - التأمين، وتجارة التجزئة، والصحة، والتعليم، والتمويل، وأكثر من ذلك - حيث يتم التقاط التجربة الشخصية وحسابها سرا للتنبؤات السلوكية المختلفة. في الوقت الحالي، ليس من قبيل المبالغة القول إن الإنترنت مملوك ويديره رأس مال مراقبة خاص.

في التنافس على اليقين، علم الرأسماليون أن أكثر البيانات التنبئية تأتي ليس فقط من المراقبة ولكن أيضًا من تعديل السلوك وتوجيهه. على سبيل المثال، بحلول عام 2013، تعلّم Facebook كيفية هندسة الإشارات المموهة على صفحاته لتشكيل تصرفات المستخدمين في العالم الواقعي ومشاعرهم. في وقت لاحق، تم الجمع بين هذه الأساليب مع التحليلات العاطفية في الوقت الحقيقي، مما يسمح للمسوقين لإظهار السلوك في لحظة أقصى درجة من الضعف. تم الاحتفال بهذه الاختراعات لكونها فعالة وغير قابلة للكشف. أثبتت Cambridge Analytica

لاحقًا أنه يمكن استخدام نفس الأساليب لتشكيل السلوك السياسي أكثر منه التجاري. لعبة الـ (Augmented reality) الواقع المعزز Pokémon Go، التي تم تطويرها في Google وتم إصدارها في عام 2016 من قبل شركة spinoff من Google، أخذت التحدي المتمثل في التعديل السلوكي الشامل إلى مستوى جديد. دفع عملاء قطاع الأعمال من ماكدونالدز إلى ستاربكس «تكاليف» لمؤسساتهم على أساس «تكلفة لكل زيارة»، مثلما يدفع المعلنون عبر الإنترنت مقابل «تكلفة النقرة الواحدة». تعلم مهندسو اللعبة كيفية تربية الناس عبر مدنهم ومدنهم إلى وجهات التي تساهم في الأرباح، كل ذلك دون علم لاعبي اللعبة.



الصورة (17) حشد من الناس قرب برج تورنتو الشهير في كندا وهم يتجمعون للعب اللعبة الشهيرة الرقمية الـ (Pokémon Go) والتي تم استخدامها لمراقبة الحشود وسلوكيات البشر المختلفة خلالها والاستيلاء على البيانات الخاصة بهم لاستخدامها لاحقاً في إنتاج تطبيقات مماثلة لما تسمى ال- التعمية الرقمية الاجتماعية (Digital social masking).

لقد نمت الديمقراطية ظاهريًّا بينما ازدهرت رأسمالية المراقبة واقعيا. إذْ غدى أصحاب رؤوس الأموال يتمتعون بنوع من التميز فريد من نوعه في القرن الحادي والعشرين وهو أقرب للشمولية التي عرفناها منذ ما يقرب على قرن من الزمان. لنسميها «قوة صك»، فهي تنفذ إرادتها من خلال الهندسة المعمارية في كل مكان من الأجهزة الرقمية. بدلاً من الأخ الأكبر الحميم الذي يستخدم القتل والإرهاب لامتلاك كل روح من الداخل إلى الخارج، تعتبر هذه الشبكات الرقمية «الآخر الكبير»: أنظمة غير شخصية مدربة على مراقبة وتشكيل أعمالنا عن بعد، دون عوائق بموجب القانون. إن قوة تلك الأدوات سوف تجعل مستقبلنا مادة للمراقبة من قبل مصالح الرأسمالية بكل محاورها. ولكن لأن هذه القوة الجديدة لا تطالب بأجسادنا من خلال العنف والخوف، فإننا نخفف من آثارها ونخفف من حذرنا. القوة الأدواتية لا تريد أن تحطمنا؛ إنها ببساطة تريد أتمتة كاملة لنا ولوعينا الداخلي. تحقيقا لهذه الغاية، فإنه ينفينا من سلوكنا. لا يهتم بما نفكر فيه أو نشعر به أو نفعله، طالما نفكر ونشعر ونفعل الأشياء بطرق يسهل على مليارات الآخرين الحصول عليها من

عيون وآذان حساسة وفعالة كما سردها لنا بحبكة درامية فيلم الدائرة (The Circle) من تمثيل ايما واتسون وتوم هانكس في رواية تستقرئ المستقبل الذي ينتظرنا مع خصوصيتنا التي يتم انتهاكها. إذًا إن قوة تلك الأدوات الرقمية تتحدى الديمقراطية بشكل مبطن رغم الادعاء بأنها أحد أدوات التعبير الحر عن الآراء والتفكير غير المبرمج. لكن الحكومات الكبيرة الأخرى تعرف كل شيء عن تلك الأدوات، بينما تظل عملياتها مخفية عن الجمهور بشكل متعمد، مما يلغي حقنا في المقاومة والثورة. بلا شك فإن هذه الممارسة تقوض الاستقلالية البشرية وتقرير المصير الحر، والتي بدونها لا يمكن للديمقراطية البقاء على قيد الحياة. تخلق القوة الملموسة عدم تناسق غير مسبوق في المعرفة، مرتبطًا بأوقات ما قبل العصر الحديث.

معرفة الآخرين الكبار (المؤسسات الحكومية والقيادات الدولية) عن أنفسنا كبيرة للغاية ومتشعبة، لكنها غير مستخدمة لنا ولصالحنا. الآخر الكبير يعرف كل شيء عنا، بينما لا نعرف شيئًا عن ذلك. عدم توازن القوى هذا غير قانوني، لأنه ليس لدينا بعد قوانين للسيطرة عليه، لكنه معادي للديمقراطية بشكل أساسي. يدعي رأسمالية المراقبة أن أساليبهم هي عواقب حتمية للتكنولوجيا الرقمية. وهذا غير صحيح. من السهل تخيل المستقبل الرقمي دون رأسمالية المراقبة، لكن من المستحيل تخيل الرأسمالية المراقبة دون التقنيات الرقمية. إن كل ما توقعناه في نظام ألمانيا الشرقيةالـ (DDR) باعتبارها هذه الدولة الاستبدادية المطلقة بمراقبتها للسكان قد انعكس علينا في الواقع على نطاق ما تقوم به وكالة الأمن القومي. بعد سبعة عقود، يمكننا أن نحترم وفاة أورويل لرفضنا التخلي عن المستقبل الرقمي. احتقر أورويل باستمرار «غريزة الانحناء أمام غزاة هذه اللحظة». وأصر على أن الشجاعة تطالب بأن نؤكد توجهاتنا الأخلاقية، حتى ضد القوى التي تبدو أنها لا تقهر.

مثل أورويل، فكر جيدًا وانتقد. لا تأخذ الحرية أمرا مفروغا منه. ناضل من أجل فكرة واحدة في القصة الإنسانية الطويلة التي تؤكد حق الناس في حكم أنفسهم. يعتقد أورويل أنه كان يستحق الموت من أجله. ومما يزيد الأمور تعقيدًا، حقيقة أن الأساس الاقتصادي والاجتماعي لكثير من وجودنا الرقمي الحديث يتركز الآن بشكل ثابت حول شكل ما من أشكال المراقبة؛ على سبيل المثال، لا تعمل منصة الوسائط الاجتماعية مثل Facebook بالطريقة التي تعمل بها بصورة شفافة وعادلة لأن مستخدميها يسمحون للشركة بشباك بياناتهم الشخصية مقابل خدمات قائمة على التوصيات. قد لا نتعرف دائمًا على هذا الشكل الأكثر حكمة من المراقبة لما هو عليه، ولكن يُعتقد

أن انتشاره يعقد فهمنا الفرق بين تتبع البيانات الصحي والمراقبة غير الصحية. يشارك الكثير من الأشخاص الأصغر سنا معلوماتهم الشخصية يشاركونها بحرية لأن هذه هي الثقافة التي نشأوا فيها. الأشخاص الأكبر سنا قليلا، هم جدد في ذلك ويفعلون ذلك بشكل متعقل وبحذر شديد، لكنه شيء تعلموه عندما كانوا أكبر سنا وربما لديهم مسافة أكثر حرجًا حولها. «يمكن أن تتراوح تلك المسافة الحرجة (critical distance) بين «نعم، سأشارك كل شيء» وافتح الباب على مصراعيه طوال الطريق إلى الشفافية الكاملة لمعلومات الشخص المقابل: ولكن قد تلتقي بأشخاص من نوعية «أنا لا أملك حتى هاتفًا محمولًا» وعلى المستوى الشخصي لم أمتلك هاتفًا ذكيًّا فعلاً حتى عام 2016. قد تلتقي بأشخاص مثل هذا، الذين يخشون حقًّا جوانب المراقبة التي لا يمتلكونها على الهاتف المحمول. لا يمكنك القول إن هناك أي رد فعل صحيح على هذا. كل هذا لا يزال جديدا جدا. في بعض النواحي نتعلم جميعًا معًا. ما لم نوجهه حقًا هو تلك اللحظة البعيدة الحاسمة لمعرفة من يتجسس علينا. ننظر إلى الاتجاه الآخر عندما تراقبنا Google وهو التذمر والتمرد، ولكن عندما تراقبنا الحكومة من خلال أدوات تلك الشركة نفسها، فإن دمنا يبرد، وفي العام الماضي، أصبح عدد متزايد من الناس في تلك اللحظة من أصحاب الدماء الباردة الذين يخافون من مراقبة الحكومات لهم ويسلمون للأمر الواقع! هذه معضلة كبيرة، لأن المراقبة لـ Google لها مكون تجاري قوي وتضعها على خلاف مع الحكومة حيث يوجد مكون أمني... لذلك هناك توتر أساسي بين احتياجات التجارة واحتياجات أمن الدولة. »

يمكنك أن تتخيل عزيزي القارئ في المستقبل الخيالي العلمي الغريب أن وكالة الأمن القومي NSA ستحصل على بياناتها من جوجل. في الواقع، لقد تبين أن وكالة الأمن القومي كانت تستغل خلاصة بيانات Google، هذا صحيح! أو يمكنك أن تتخيل مستقبلًا مختلفًا للخيال العلمي حيث ستحصل Google على موجز بيانات NSA لتزويدك بمنتجات وخدمات أفضل. لقد ثبت بالفعل أن نصف هذا المستقبل الغريب في الخيال العلمي. إذاً لديك هذا الموقف حيث، على الرغم من أن أهدافها مختلفة تمامًا، فمن الممكن للدولة أن تخرب أهداف التجارة من أجل غاياتها الخاصة. ومع ذلك، هناك علامات واضحة على الارتداد من الشبكات الاجتماعية وموفري خدمة الاتصالات ضد الاشتراك في جهاز أمان من نظام مشابه لنظام الأورويلياني. في أحد الأوقات الماضية أعلنت شركة الاتصالات العالمية فودافون عن قلقها إزاء الطبيعة الزاحفة للمراقبة الأمنية الحكومية للكثير من العملاء لديها. أصدرت المنظمة ما أسماه «تقرير الكشف عن قوة إنفاذ القانون» متهماً الحكومات

بجمع القوى الفكرية والاجتماعية للمساعدة في الإقناع بالضغط على مقدمي الخدمات عبر الإنترنت إلى التعاون في مجال المراقبة الأمنية واختراق البيانات الشخصية لعدد من المواطنين. وبكل تأكيد لا ترغب شركات التكنولوجيا في أن تكون الوكيل للحكومة وبعد ذلك تتحمل المسؤولية عن أي مراقبة تحدث، بغض النظر عن مدى شرعيتها.

النهاية

المصادر والبحوث

Ahmed, A.; Krishnan, V. V. G.; Foroutan, S. A.; Touhiduzzaman,• M.; Rublein, C.; Srivastava, A.; Wu, Y.; Hahn, A. & Suresh, S. (2019), ‘Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems’, IEEE Transactions on Industry Applications 55(6), 6313- 6323.

Bakici, S.; Erkek, B.; Manti, V. & Altekin, A. (2017), ‘TRUSTED• DATA COMMUNICATION AND SECURITY ISSUES IN GNSS NETWORK OF TURKEY’, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences XLII-4-W6, 23- 26.

Bhat, K.; Sundarraj, V.; Sinha, S. & Kaul, A. (2013), ‘IEEE Cyber • Security for the Smart Grid’, IEEE Cyber Security for the Smart Grid, 1- 122.

Cha, S. & Yeh, K. (2018), ‘A Data-Driven Security Risk • Assessment Scheme for Personal Data Protection’, IEEE Access 6, 50510-50517.

Chen, Y. R.; Sha, J. R. & Zhou, Z. H. (2019), ‘IOV Privacy • Protection System Based on Double-Layered Chains’, Wireless Communications and Mobile Computing 2019.

Cristian, I. R.; Ioana, C. & Cristian, I. (2018), 'Considerations on • the implementation steps for an information security management system', Proceedings of the International Conference on Business Excellence 12(1), 476- 485.

Đekić Milica, D. (2016), 'Cyber procedures for a business • environment in Serbia', Tehnika 71(3), 471- 474.

Dong, Q.; Chen, M.; Li, L. & Fan, K. (2018), 'Cloud-based radio • frequency identification authentication protocol with location privacy protection', International Journal of Distributed Sensor Networks 14.

Dragan, T.; Olja, A. & Edita, K. (2016), 'Management of • organizations in Serbia from the aspect of the maturity analysis of information security', International Review 2016(3-4), 42- 50.

Dragan, Đ. & Miroslav, S. (2017), 'Internet as a method of trolling • offensive intelligence operations in cyberspace', NBP: Nauka, bezbednost, policija 22(2), 13- 32.

Drugan, T. C. & ISTRATE, D. (2019), 'Patient data security in the • era of medical connected devices', Applied Medical Informatics 41(Suppl. 1).

Fantacci, R.; Nizzi, F.; Pecorella, T.; Pierucci, L. & Roveri, M. • (2019), 'False Data Detection for Fog and Internet of Things Networks', Sensors 19(19), 4235.

Ferreira, M. R. & Kawakami, C. (2018), 'Ransomware-Kidnapping • personal data for ransom and the information as hostage', Advances in Distributed Computing and Artificial Intelligence Journal 7(3), 5- 14.

Giarratano, D.; Guise, L. & Bodin, J. (2017), 'Does cyber security • moving towards risk management leads to new grid organisation?', CIRED-Open Access Proceedings Journal 2017(1), 2700- 2702.

Grachkov, I. A. & Malyuk, A. A. (2019), 'Development problems of • trusted software applied at critical information infrastructure objects (organizational and methodological aspects)', Bezopasnost′ Informacionnyh Tehnologij 26(1), 56- 63.

Hingant, J.; Zambrano, M.; Pérez, F. J.; Pérez, I. & Esteve, M. • (2018), 'HYBINT: A Hybrid Intelligence System for Critical Infrastructures Protection', Security and Communication Networks 2018.

Hong, J.; Nuqui, R. F.; Kondabathini, A.; Ishchenko, D. & Martin, • and Circuit BreakerA. (2019), 'Cyber Attack Resilient Distance Protection Control for Digital Substations', IEEE Transactions on Industrial Informatics 15(7), 4332- 4341.

Hossain-McKenzie, S.; Kazerooni, M.; Davis, K.; Etigowni, S. & • Zonouz, S. (2017), 'Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment', IET Cyber-Physical Systems.

Ibrahimi, S.; Dervishi, E. & Ibrahimi, E. (2018), 'Cyberdeviance • and the Role of Data Privacy Officer's Sustainable Structures in its Prevention', Open Journal for Psychological Research 2(2), 61- 68.

Iturbe, M.; Garitano, I.; Zurutuza, U. & Uribeetxeberria, R. (2017), • 'Towards Large-Scale, Heterogeneous Anomaly Detection Systems in

Industrial Networks: A Survey of Current Trends', Security and Communication Networks 2017.

Ivanova, X. A. (2019), 'Online voting as an element of • cybersecurity of megacities', Pravoprimenenie 3(2), 31- 37.

Kamarudin, M. H.; Maple, C.; Watson, T. & Safa, N. S. (2017), 'A • New Unified Intrusion Anomaly Detection in Identifying Unseen Web Attacks', Security and Communication Networks 2017.

Kandeh, A. T.; Botha, R. A. & Futcher, L. A. (2018), 'Enforcement • Perspective of dataof the Protection of Personal Information (POPI) Act: management professionals', South African Journal of Information Management 20(1), e1- e9.

Kobek, L. P. & Caldera, E. (2016), 'Cyber Security and Habeas • Data: The Latin American response to information security and data protection', OASIS 0(24), 109- 128.

Konstantinou, C.; Sazos, M.; Musleh, A. S.; Keliris, A.; Al-Durra, • A. & Maniatakos, M. (2017), 'GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment', IET Cyber-Physical Systems.

Kure, H. I. & Islam, S. (2019), 'Assets focus risk management • framework for critical infrastructure cybersecurity risk management', IET Cyber-Physical Systems.

Lian, H.; Qiu, W.; Yan, D.; Huang, Z. & Guo, J. (2017), 'Efficient • Privacy-Preserving Protocol for k-NN Search over Encrypted Data in

Location-Based Service', Complexity 2017.

van der Linden Dirk; Matthew, E.; Irit, H. & Anna, Z. (2020), 'Pets • without PETs: on pet owners' under-estimation of privacy concerns in pet wearables', Proceedings on Privacy Enhancing Technologies 2020(1), 143-164.

Liu, X.; Shahidehpour, M.; Li, Z.; Liu, X.; Cao, Y. & Li, Z. (2017), • 'Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems', IEEE Transactions on Smart Grid 8(2), 572- 580.

Liu, N.; Zang, W.; Chen, S.; Yu, M. & Sandhu, R. (2019), 'Adaptive • Noise Injection against Side-Channel Attacks on ARM Platform', EAI Endorsed Transactions on Security and Safety 6(19).

Liu, S.; Liang, C.; Wang, L.; Zeng, L. & Wang, C. (2019), • 'Variation Characteristics of the Main Hydrochemical Indexes in Typical Subterranean Rivers in the South China Karst Region Based on Curve Fitting', The Scientific World Journal 2019.

Marek, P. (2019), 'Concept of the railway safety, security and • cybersecurity functional integrity levels', MATEC Web of Conferences 294, 03003.

Min, Z.; Yang, G.; Sangaiah, A. K.; Bai, S. & Liu, G. (2019), 'A • privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems', EURASIP Journal on Wireless Communications and Networking 2019(1), 1- 14.

Nawari, N. O. & Ravindran, S. (2019), 'Blockchain and Building • Information Modeling (BIM): Review and Applications in Post-Disaster Recovery', Buildings 9(6), 149.

Nenad, P.; Mladen, M. & Vladimir, C. (2013), 'The protection of • educational institutions from cyber crime and cyberbullying: Problems and dilemmas', Sociološki Pregled 47(1), 75- 92.

Obitade, P. O. (2019), 'Big data analytics: a link between knowledge • management capabilities and superior cyber protection', Journal of Big Data 6(1), 1- 28.

Ogigau-Neamtiu, F. (2017), 'AUTOMATING THE DATA • SECURITY PROCESS', Journal of Defense Resources Management 8(2), 91- 100.

Pal, S.; Hitchens, M.; Varadharajan, V. & Rabehaja, T. (2018), • 'Fine-Grained Access Control for Smart Healthcare Systems in the Internet of Things', EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 4(13).

Pesic, G. S. (2018), 'Surviving and Thriving in the Digital • Economy', The School of Public Policy Publications 11(11), 1- 14.

PETROIA, A. & Ivan, B. A. N. U. (2019), 'THE RISKS OF • CYBERSECURITY OF FINANCIAL INSTITUTIONS AND POSSIBLE METHODS FOR THEIR ELIMINATION*', Economica 4(110), 156- 163.

R.Rahman, M. S.; Mahmud, M. A.; Oo, A. M. T. & Pota, H. • (2017), 'Multi-Agent Approach for Enhancing Security of Protection

Schemes in Cyber-Physical Energy Systems', IEEE Transactions on Industrial Informatics 13(2), 436- 447.

Ramos, J. L. H.; Geneiatakis, D.; Kounelis, I.; Steri, G. & Fovino, I. • N. (2020), 'Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies', IEEE Security & Privacy 18(1), 28- 38.

Rangu, C. A. L. I. N. M. & Badea, L. (2019), 'Cyber-risk insurance- • a big challenge facing contemporary economies', Revista de Studii Financiare 4(6), 10- 33.

Rudinskiy, I. D. & Okolot, D. Y. (2019), 'Social networks of • educational purpose as a subject of protection in the preparation of specialists of information security', Otkrytoe Obrazovanie (Moskva) 23(1), 46- 56.

Ryan, M. (2018), 'Ethics of Public Use of AI and Big Data', ORBIT • Journal 2(1).

Skrynkovskyy, R.; Pawlowski, G.; Harasym, P. & Koropetskyi, O. • (2017), 'Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise', Traektoriâ Nauki 3(10), 5001- 5009.

Tso, R.; Liu, Z.-Y. & Hsiao, J.-H. (2019), 'Distributed E-Voting and • 8(4), 422.E-Bidding Systems Based on Smart Contract', Electronics

Tsochev, G. R.; Yoshinov, R. D. & Iliev, O. P. (2019), 'Key • Problems of the Critical Information Infrastructure through Scada Systems Research', Труды СПИИРАН 18(6), 1333- 1356.

Wahyudi, W. (2019), 'INVESTOR LEGAL PROTECTION IN THE • INDONESIAN INDUSTRIAL 4.0', Tadulako Law Review 4(2), 216- 227.

Wang, C.; Zheng, Y.; Jiang, J. & Ren, K. (2018), 'Toward Privacy- • Preserving Personalized Recommendation Services', Engineering 4(1), 21-28.

Wang, Q.; Tai, W.; Tang, Y. & Ni, M. (2019), 'Review of the false • data injection attack against the cyber-physical power system', IET Cyber-Physical Systems.

Yang, J.; Zhou, C.; Yang, S.; Xu, H. & Hu, B. (2018), 'Anomaly • Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems', IEEE Transactions on Industrial Electronics 65(5), 4257- 4267.

Yin, X. C.; Liu, Z. G.; Ndibanje, B.; Nkenyereye, L. & Islam, S. M. • R. (2019), 'An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks', Sensors 19(14), 3146.

Kostopoulos, G. K. (2013), Cyberspace and cybersecurity, CRC • Press, Boca Raton, Fla. [u.a.].

Taplin, R., ed. (2016), Managing cyber risk in the financial sector, • Routledge, London.

Adlakha, R.; Sharma, S.; Rawat, A. & Sharma, K. (2019), Cyber • Security Goal's, Issue's, Categorization Data Breaches, in 'Proc. Cloud and Parallel Computing (COMITCon) 2019 Int. Conf. Machine Learning, Big Data', pp. 397- 402.

Ahmed, A.; Krishnan, V. V. G.; Foroutan, S. A.; Touhiduzzaman, •
M.; Srivastava, A.; Wu, Y.; Hahn, A. & Sindhu, S. (2018), Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems, in 'Proc. IEEE Industry Applications Society Annual Meeting (IAS)', pp. 1- 8.

Anatoliy, P. N.; Kristina, V. A.; Elena, A. K.; Vagiz, D. G. & •
Aleksandr, V. S. (2018), Technologies of safety in the bank sphere from cyber attacks, in 'Proc. IEEE Conf. of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)', pp. 102- 104.

Babun, L.; Aksu, H. & Uluagac, A. S. (2016), A framework for •
counterfeit smart grid device detection, in 'Proc. IEEE Conf. Communications and Network Security (CNS)', pp. 382- 383.

Carolin, S. P. & Somasundaram, M. (2016), Data loss protection and •
data security using agents for cloud environment, in 'Proc. Int. Conf. Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)', pp. 1- 5.

Chen, H.; Chen, X.; Fan, L. & Chen, C. (2015), Classified security •
protection evaluation for vehicle information system, in 'Proc. Industrial Control System and Communications (SSIC) 2015 Int. Conf. Cyber Security of Smart Cities', pp. 1- 6.

Chen, H.; Hu, M.; Yan, H. & Yu, P. (2019), Research on Industrial •
Internet of Things Security Architecture and Protection Strategy, in 'Proc. Int. Conf. Virtual Reality and Intelligent Systems (ICVRIS)', pp. 365- 368.

Coats, D. & Nuqui, R. (2018), Method for Detecting Intrusive •
Sensor Data by Enhanced Multi-Terminal Differential Protection, in 'Proc.

IEEE/PES Transmission and Distribution Conf. and Exposition (T D)', pp. 1- 5.

Fan, X.; Fan, K.; Wang, Y. & Zhou, R. (2015), Overview of cyber- • security of industrial control system, in 'Proc. Industrial Control System and Communications (SSIC) 2015 Int. Conf. Cyber Security of Smart Cities', pp. 1- 7.

Fan, W.; Ziembicka, J.; de Lemos, R.; Chadwick, D.; Cerbo, F. D.; • Privacy-PreservingSajjad, A.; Wang, X. & Herwono, I. (2019), Enabling Sharing of Cyber Threat Information in the Cloud, in 'Proc. 6th IEEE Int. Conf. Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE Int. Conf. Edge Computing and Scalable Cloud (EdgeCom)', pp. 74- 80.

Farion, A.; Dluhopolskyi, O.; Banakh, S.; Moskaliuk, N.; Farion, M. • & Ivashuk, Y. (2019), Using blockchain Technology for Boost Cyber Security, in 'Proc. 9th Int. Conf. Advanced Computer Information Technologies (ACIT)', pp. 452- 455.

Farquharson, J.; Wang, A. & Howard, J. (2012), Smart Grid Cyber • Security and substation Network Security, in 'Proc. IEEE PES Innovative Smart Grid Technologies (ISGT)', pp. 1- 5.

Fontenele, M. & Sun, L. (2016), Knowledge management of cyber • security expertise: an ontological approach to talent discovery, in 'Proc. Int. Conf. On Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 13.

Frattini, F.; Giordano, U. & Conti, V. (2019), Facing Cyber-Physical • Security Threats by PSIM-SIEM Integration, in 'Proc. 15th European

Dependable Computing Conf. (EDCC)', pp. 83- 88.

Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M. & •
Naqvi, S. A. (2018), The Good, the Bad and the Ugly: A Study of Security
in 'Proc. IEEE/ACM 40th Int.Decisions in a Cyber-Physical Systems Game,
Conf. Software Engineering (ICSE)', pp. 496.

Godse, V. (2010), Building an Ecosystem for Cyber Security and •
Data Protection in India, in Ajay Kumar & David Zhang, ed., 'Ethics and
Policy of Biometrics-Third International Conference on Ethics and Policy of
Biometrics and International Data Sharing, ICEB 2010, Hong Kong, January
4-5, 2010. Revised Papers', Springer, pp. 138- 145.

Gruschka, N.; Mavroeidis, V.; Vishi, K. & Jensen, M. (2018), •
Privacy Issues and Data Protection in Big Data: A Case Study Analysis under
GDPR, in 'Proc. IEEE Int. Conf. Big Data (Big Data)', pp. 5027- 5033.

Gurnani, R.; Pandey, K. & Rai, S. K. (2014), A scalable model for •
implementing Cyber Security Exercises, in 'Proc. Int. Conf. Computing for
Sustainable Global Development (INDIACom)', pp. 680- 684.

Haoyu, W. (2012), Privacy, How Can I Protect You? How to •
Construct Safe Data Security System in E-commerce Transaction, in 'Proc.
Fourth Int. Conf. Computational and Information Sciences', pp. 441- 444.

Hooper, E. (2009), Intelligent strategies and techniques for effective •
in 'Proc. (ICITST) 2009cyber security, infrastructure protection and privacy,
Int. Conf. for Internet Technology and Secured Transactions', pp. 1- 7.

Huang, C. (2015), Security system and actual operation benefit of • data transmission on heterogeneous network, in 'Proc. Int. Carnahan Conf. Security Technology (ICCST)', pp. 165- 168.

Hurst, W.; Merabti, M. & Fergus, P. (2014), Big Data Analysis • Techniques for Cyber-threat Detection in Critical Infrastructures, in 'Proc. 28th Int. Conf. Advanced Information Networking and Applications Workshops', pp. 916- 921.

Jayanthi, M. K. (2017), Strategic Planning for Information Security- • DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom, in 'Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)', pp. 142- 147.

Kabiri, P. & Chavoshi, M. (2019), Destructive Attacks Detection • and Response System for Physical Devices in Cyber-Physical Systems, in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 6.

Kang, M. & Kwon, H. (2019), A Study on the Needs for • Enhancement of Personal Information Protection in Cloud Computing Security Certification System, in 'Proc. Int. Conf. Platform Technology and Service (PlatCon)', pp. 1- 5.

Kannan, M. K. J. (2017), A bird's eye view of Cyber Crimes and • Free and Open Source Software's to Detoxify Cyber Crime Attacks-an End User Perspective, in 'Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)', pp. 232- 237.

Kapusta, K.; Memmi, G. & Noura, H. (2017), Secure and resilient • scheme for data protection in unattended wireless sensor networks, in 'Proc.

1st Cyber Security in Networking Conf. (CSNet)', pp. 1- 8.

Kim, Y.; Moon, I. & Lee, S. (2016), A design of cyber security •
testbed for DPPS and PMAS in Korean operating nuclear power plant, in 'Proc. Automation and Systems (ICCAS) 2016 16th Int. Conf. Control', pp. 1480- 1483.

Kim, J.; Kim, K. & Jang, M. (2019), Cyber-Physical Battlefield •
Platform for Large-Scale Cybersecurity Exercises, in 'Proc. 11th Int. Conf. Cyber Conflict (CyCon)', pp. 1- 19.

Koch, A.; Altschaffel, R.; Kiltz, S.; Hildebrandt, M. & Dittmann, J. •
(2018), Exploring the Processing of Personal Data in Modern Vehicles-A Proposal of a Testbed for Explorative Research to Achieve Transparency for Privacy and Security, in 'Proc. 11th Int. Conf. IT Security Incident Management IT Forensics (IMF)', pp. 15- 26.

Kohli, S. (2016), Developing Cyber Security Asset Management •
framework for UK rail, in 'Proc. Data Analytics And Assessment (CyberSA) 2016 Int. Conf. On Cyber Situational Awareness', pp. 1- 6.

Kotenko, I. (2007), Multi-agent Modelling and Simulation of •
Cyber-Attacks and Cyber-Defense for Homeland Security, in 'Proc. 4th IEEE Workshop Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications', pp. 614- 619.

Kotenko, I. & Novikova, E. (2014), Visualization of Security •
Metrics for Cyber Situation Awareness, in 'Proc. Reliability and Security 2014 Ninth Int. Conf. Availability', pp. 506- 513.

Kotenko, I. V.; Levshun, D. S. & Chechulin, A. A. (2016), Event • correlation in the integrated cyber-physical security system, in 'Proc. XIX IEEE Int. Conf. Soft Computing and Measurements (SCM)', pp. 484- 486.

League, S. J. (1997), Critical Infrastructure Protection-the • cyber/information dimension: report on national infrastructure coordination initiatives, in 'Proc. 13th Annual Computer Security Applications Conf', pp. 118- 120.

Lee, H.; Lee, K. & Won, D. (2011), Protection Profile of Personal • Information Security System: Designing a Secure Personal Information Computing andSecurity System, in 'Proc. Security and Privacy in Communications 2011IEEE 10th Int. Conf. Trust', pp. 806- 811.

Lee, M. G. (2012), Securing the human to protect the system: • Human factors in cyber security, in 'Proc. incorporating the Cyber Security Conf 7th IET Int. Conf. System Safety 2012', pp. 1- 5.

Qian, L. (2013), Study of information system security of • government data center based on the classified Protection, in 'Proc. 8th Int. Conf. Computer Science Education', pp. 1315- 1319.

Litherland, M. & Bross, M. (2013), From civil to cyber rights: A • perspective on cyber policy challenges in our connected world, in 'Proc. World Cyberspace Cooperation Summit IV (WCC4)', pp. 1- 4.

Liu, Y.; Qin, H.; Chen, Z.; Shi, C.; Zhang, R. & Chen, W. (2019), • Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant, in 'Proc. IEEE Int. Conf. Energy Internet (ICEI)', pp. 25- 30.

Lu, Z. (2016), Research about New Media Security Technology •
Base on Big Data Era, in ‘Proc. nd Intl Conf Big Data Intelligence and Computing and Cyber Science and Technology
14th Intl ConfCongress(DASC/PiCom/DataCom/CyberSciTech) 2016 IEEE Dependable, Autonomic and Secure Computing, 14th Intl Conf Pervasive Intelligence and Computing’, pp. 933- 936.

Lundgren, M. & Bergström, E. (2019), Security-Related Stress: A •
Perspective on Information Security Risk Management, in ‘Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)’, pp. 1- 8.

Montefusco, P.; Casar, R.; Koelle, R. & Stelkens-Kobsch, T. H. •
(2016), Addressing Security in the ATM Environment: From Identification to Validation of Security Countermeasures with Introduction of New Security Capabilities in the ATM System Context, in ‘Proc. Reliability and Security (ARES) 2016 11th Int. Conf. Availability’, pp. 532- 541.

Nikolopoulos, D.; Makropoulos, C.; Kalogeras, D.; Monokrousou, •
K. & Tsoukalas, I. (2018), Developing a Stress-Testing Platform for Cyber-Physical Water Infrastructure, in ‘Proc. Int. Workshop Cyber-Physical Systems for Smart Water Networks (CySWater)’, pp. 9- 11.

Nuqui, R.; Hong, J.; Kondabathini, A.; Ishchenko, D. & Coats, D. •
(2018), A Collaborative Defense for Securing Protective Relay Settings in Electrical Cyber Physical Systems, in ‘Proc. Resilience Week (RWS)’, pp. 49- 54.

Ogbu, J. O. & Oksiuk, A. (2016), Information protection of data •
processing center against cyber attacks, in ‘Proc. Third Int. Scientific-

Practical Conf. Problems of Info-communications Science and Technology (PIC S T)', pp. 132- 134.

Onwubiko, C. (2016), Exploring web analytics to enhance cyber • situational awareness for the protection of online web services, in 'Proc. Int. Conf. On Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 8.

Onwubiko, C. (2017), Security operations centre: Situation • awareness, threat intelligence and cybercrime, in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 6.

Onwubiko, C. & Ouazzane, K. (2019), Cyber Onboarding is • 'Broken', in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 13.

Onyigwang, O. J.; Shestak, Y. & Oksiuk, A. (2016), Information • protection of data processing center against cyber attacks, in 'Proc. IEEE First Int. Conf. Data Stream Mining Processing (DSMP)', pp. 397- 400.

Panjwani, M. & Jäntti, M. (2017), Data Protection Security • Challenges in Digital IT Services: A Case Study, in 'Proc. Int. Conf. Computer and Applications (ICCA)', pp. 379- 383.

Peng, Y.; Huang, K.; Tu, W. & Zhou, C. (2018), A Model-Data • Integrated Cyber Security Risk Assessment Method for Industrial Control Systems, in 'Proc. IEEE 7th Data Driven Control and Learning Systems Conf. (DDCLS)', pp. 344- 349.

Qiang, L.; Zhengwei, J.; Zeming, Y.; Baoxu, L.; Xin, W. & Yunan, •
Z. (2018), A Quality Evaluation Method of Cyber Threat Intelligence in User Perspective, in 'Proc. Security And Privacy In Computing And Communications/ 12th IEEE Int 2018 17th IEEE Int. Conf. On Trust Conf. On Big Data Science and Engineering (TrustCom/BigDataSE)', pp. 269- 276.

Rajamäki, J. & Pirinen, R. (2015), Critical Infrastructure Protection: •
Towards a Design Theory for Resilient Software-Intensive Systems, in 'Proc. European Intelligence and Security Informatics Conf', pp. 184.

Reed, J. H. & Gonzalez, C. R. A. (2012), Enhancing Smart Grid •
cyber security using power fingerprinting: Integrity assessment and intrusion detection, in 'Proc. Future of Instrumentation Int Workshop (FIIW)', pp. 1- 3.

Romanski, G. (2012), Combined safety and security certification, in •
'Proc. incorporating the Cyber Security Conf 7th IET Int. Conf. System Safety 2012', pp. 1- 5.

Features-Romansky, R. & Noninska, I. (2019), Cyber Space •
Security and Data Protection Requirements, in 'Proc. Int. Conf. Information Technologies (InfoTech)', pp. 1- 4.

Sanjab, A. & Saad, W. (2016), On bounded rationality in cyber- •
physical systems security: Game-theoretic analysis with application to smart grid protection, in 'Proc. Joint Workshop Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)', pp. 1- 6.

Scharnick, N.; Gerber, M. & Futcher, L. (2016), Review of data •
storage protection approaches for POPI compliance, in 'Proc. Information Security for South Africa (ISSA)', pp. 48- 55.

Scheper, C.; Cantor, S. & Karlsen, R. (2009), Trusted Distributed • Repository of Internet Usage Data for Use in Cyber Security Research, in 'Proc. Cybersecurity Applications Technology Conf. for Homeland Security', pp. 83- 88.

Sedinic, I.; Lovric, Z. & Perusic, T. (2014), Customer and user • education as a tool to increase security level, in 'Proc. Electronics and Microelectronics (MIPRO) 2014 37th Int. Convention Information and Communication Technology', pp. 1441- 1445.

Seker, E. & Ozbenli, H. H. (2018), The Concept of Cyber Defence • Exercises (CDX): Planning, Execution, Evaluation, in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 9.

Sevis, K. N. & Seker, E. (2016), Cyber warfare: terms, issues, laws • and controversies, in 'Proc. Int. Conf. On Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 9.

Sharafeev, T. R.; Ju, O. V. & Kulikov, A. L. (2018), Cyber-Security • Problems in Smart Grid Cyber Attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems, in 'Proc. Applications and Manufacturing (ICIEAM) 2018 Int. Conf. Industrial Engineering', pp. 1- 6.

Shukla, M.; Johnson, S. D. & Jones, P. (2019), Does the NIS • implementation strategy effectively address cyber security risks in the UK? in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 11.

Sindhusha, P. & Bharathi, B. (2017), Privacy protection on data • overflow system for smartphones, in 'Proc. Energy Information and

Commuincation (ICCPEIC) 2017 Int. Conf. Computation of Power', pp. 310-315.

Skinner, G. (2016), Cyber security for younger demographics: A • graphic based authentication and authorisation framework, in 'Proc. IEEE Region 10 Conf. (TENCON)', pp. 2487- 2490.

Skopik, F.; Wurzenberger, M.; Settanni, G. & Fiedler, R. (2015), • Establishing national cyber situational awareness through incident Assessment (CyberSA)information clustering, in 'Proc. Data Analytics and 2015 Int. Conf. Cyber Situational Awareness', pp. 1- 8.

Skopik, F. & Filip, S. (2019), Design principles for national cyber • security sensor networks: Lessons learned from small-scale demonstrators, in 'Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)', pp. 1- 8.

Slipachuk, L.; Toliupa, S. & Nakonechnyi, V. (2019), The Process • of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Managem ent in Ukraine, in 'Proc. 3rd Int. Conf. Advanced Information and Communications Technologies (AICT)', pp. 451- 454.

Soupionis, Y. & Benoist, T. (2014), Demo abstract: Demonstrating • cyber-attacks impact on cyber-physical simulated environment, in 'Proc. ACM/IEEE Int. Conf. Cyber-Physical Systems (ICCPS)', pp. 222.

Soupionis, Y. & Benoist, T. (2015), Cyber-physical testbed-The • impact of cyber attacks and the human factor, in 'Proc. 10th Int. Conf. for Internet Technology and Secured Transactions (ICITST)', pp. 326- 331.

Soupionis, Y.; Piccinelli, R. & Benoist, T. (2016), Cyber security •
Federated Conf.impact on power grid including nuclear plant, in 'Proc.
Computer Science and Information Systems (FedCSIS)', pp. 767- 773.

Span, M. T.; Mailloux, L. O.; Grimaila, M. R. & Young, W. B. •
(2018), A Systems Security Approach for Requirements Analysis of Complex
Cyber-Physical Systems, in 'Proc. Int. Conf. Cyber Security and Protection of
Digital Services (Cyber Security)', pp. 1- 8.

Su, S.; Duan, X.; Zeng, X.; Chan, W. L. & Li, K. K. (2007), Context •
Information based Cyber Security Defense of Protection System, in 'Proc.
IEEE Power Engineering Society General Meeting', pp. 1.

Thuraisingham, B. (2003), Data mining and cyber security, in 'Proc. •
.-Third Int. Conf. Quality Software', pp. 2

Thuraisingham, B. (2011), Data Mining for Malicious Code •
Detection and Security Applications, in 'Proc. European Intelligence and
Security Informatics Conf', pp. 4- 5.

Vegh, L. & Miclea, L. (2016), Secure and efficient communication •
in cyber-physical systems through cryptography and complex event
processing, in 'Proc. Int. Conf. Communications (COMM)', pp. 273- 276.

von Solms, S. (2013), Parliamentary oversight of Cyber Security •
Countries, in 'Proc.and Critical Information Infrastructures in Developing
Science and Information Conf', pp. 335- 339.

Vuksanović, I. P. (2019), Analysis of Possibilities for the •
Establishment and Implementation of Cyber Security in the Republic of

Croatia, in ‘Proc. Int. Symp. ELMAR’, pp. 155- 158.

Wang, L.; Mander, T.; Cheung, H.; Nabhani, F. & Cheung, R. •
(2007), Security Operation Modes for Enhancement of Utility Computer Network Cyber-Security, in ‘Proc. IEEE Power Engineering Society General Meeting’, pp. 1- 8.

Wang, Y.; Zhang, B.; Lin, W. & Zhang, T. (2011), Smart grid •
information security-a research on standards, in ‘Proc. Int. Conf. Advanced Power System Automation and Protection’, pp. 1188- 1194.

Wang, P.; Ali, A. & Kelly, W. (2015), Data security and threat •
modeling for smart city infrastructure, in ‘Proc. Industrial Control System and Communications (SSIC) 2015 Int. Conf. Cyber Security of Smart Cities’, pp. 1- 6.

Wibowo, S. (2018), Enriching Digital Government Readiness •
Indicators of RKCI Assessment with Advance Https Assessment Method to Promote Cyber Security Awareness Among Smart Cities in Indonesia, in ‘Proc. Int. Conf. ICT for Smart Society (ICISS)’, pp. 1- 4.

Xu, X.; Liu, G. & Zhu, J. (2016), Cloud Data Security and Integrity •
Protection Model Based on Distributed Virtual Machine Agents, in Bin Xie & Xiaolong Xu, ed., ‘International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2016, Chengdu, China,
, pp. 6- 13.‹October 13-15, 2016’, IEEE

Yahya, F.; Walters, R. J. & Wills, G. B. (2016), Goal-based security •
components for cloud storage security framework: a preliminary study, in

‘Proc. Int. Conf. On Cyber Security and Protection of Digital Services (Cyber Security)’, pp. 1- 5.

Yunfei, L.; Yuanbao, C.; Xuan, W.; Xuan, L. & Qi, Z. (2015), A •
Framework of Cyber-Security Protection for Warship Systems, in ‘Proc. Sixth Int. Conf. Intelligent Systems Design and Engineering Applications (ISDEA)’, pp. 17- 20.

Zgraggen, R. R. (2019), Cyber Security Supervision in the •
Insurance Sector: Smart Contracts and Chosen Issues, in ‘Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security)’, pp. 1- 4.

(2016), ‘2016 International Conference on Cyber Security and •
Protection of Digital Services (Cyber Security)’.

(2017), ‘2017 International Conference on Cyber Security and •
Protection of Digital Services (Cyber Security)’, IEEE, [Piscataway, NJ], Literaturangaben.

Al, H. Ş. E. (), ‘Cyber Security Analysis of Turkey’. •

Alberts, D. S.; Garstka, J. J. & Stein, F. P. (1999), ‘Network Centric •
Warfare: Developing and Leveraging Information Superiority’.

Alothman, B. (2019), ‘Raw Network Traffic Data Preprocessing and •
Preparation for Automatic Analysis’.

Al-Shaer, E. (2016), ‘Security and Resiliency Analytics for Smart •
Grids’(67), in Mohammad Ashiqur Rahman, ed., Springer International Publishing, Cham, Description based upon print version of record.

Bachrach, D. G. (2014), '10 don'ts on our digital devices', in Eric J. • Rzeszut, ed., Apress, Berkeley, CA, Includes index.

(2012), 'Cyber security policy guidebook', in Jennifer L. Bayuk; • Jason Healey; Paul Rohmeyer; Marcus H. Sachs; Jeffrey Schmidt & Joseph Weiss, ed., John Wiley & Sons, Hoboken, Description based upon print version of record.

Bernard, R. (2015), 'Security Technology Convergence Insights', • Elsevier Science, Burlington, Description based upon print version of record.

Calder, A. (2015), 'IT Governance', in Steve Watkins, ed.,, Kogan • Page, London, Description based upon print version of record.

Jan(2011), 'Open research problems in network security'(6555), in • Camenisch; Valentin Kisimov & Maria Dubovitskaya, ed., Springer, Berlin [u.a.], Literaturangaben.

Canavan, T. (2011), 'CMS security handbook', in David A. Chapa, • ed., Wiley Pub, Indianapolis, Ind, Includes index.

Carayannis, E. G. (2014), 'Cyber-Development, Cyber-Democracy • and Cyber-Defense', in David F. J. Campbell & Marios Panagiotis Efthymiopoulos, ed., Springer New York, New York, NY, Description based upon print version of record.

Channon, M. (2019), 'Cyber security and data protection', 47-63. •

Cole, E. (2012), 'Advanced Persistent Threat', Elsevier Science, • Burlington, Description based upon print version of record.

Conklin, W. A. (), ‘Security in Cyber-Physical Systems’. •

Copeland, M. (2017), ‘Cyber Security on Azure’, Apress, Berkeley, • CA.

Cyber Security, C. I. (2008), ‘Approach to Cyber Security’. •

Dedek, T. (2013), ‘Hardware Acceleration for Cyber Security’. •

Dodge, R. C. (2013), ‘Information Assurance and Security • Education and Training’(406), in Lynn Futcher, ed., Springer Berlin Heidelberg, Berlin, Heidelberg.

Goutam, R. K. (2009), ‘Importance of Cyber Security’. •

Guitton, C. (2017), ‘Foiling cyber attacks’. •

Hooper, D. E.; Scholar, S. & Scholar, H.-m.-y. C. (2011), ‘Cyber, • Broadband and Intelligent Security’.

Howard, D. & Prince, K. (2011), ‘Security 2020’, Wiley Pub, • Indianapolis, Ind, Includes index.

Jacobs, S. (2011), ‘Engineering information security’(v.13), Wiley- • IEEE Press, Hoboken, N.J, Includes index.

Jajodia, S. (2008), ‘Proceedings of The Ifip Tc 11 23rd International • Information Security Conference’(278), in Stelvio Cimato; Stelvio Cimato; , Springer‹Sushil Jajodia; Pierangela Samarati & Pierangela Samarati, ed. Science+Business Media, LLC, Boston, MA, Includes bibliographical references and index.

(2010), ‘Cyber Situational Awareness’(46), in Sushil Jajodia, ed., •
Springer, New York [u.a.], Includes bibliographical references and index.

(2013), ‘Moving target defense II’(100), in Sushil Jajodia; Anup K. •
Ghosh; V. S. Subrahmanian; Vipin Swarup; Cliff Wang & X. Sean Wang, ed.,
Springer, New York, NY, Description based upon print version of record.

V.(2015), ‘Cyber warfare’(56), in Sushil Jajodia; Paulo Shakarian; •
S. Subrahmanian; Vipin Swarup & Cliff Wang, ed., Springer, Cham [u.a.],
Description based upon print version of record.

Kapoor, B. & Pandya, P. (2014), ‘Data Encryption’, 29-73. •

Kremer, J.-F. (2014), ‘Cyberspace and International Relations’, in •
Benedikt Müller, ed., Springer Berlin Heidelberg, Berlin, Heidelberg,
Includes bibliographical references and index.

(2015), ‘Cyber security: analytics, technology and automation’(78), •
in Martti Lehto & Pekka Neittaanmäki, ed., Springer, Cham, Description
based upon print version of record.

Loukas, G. (2015), ‘Cyber-physical attacks’, Elsevier Science, •
Burlington, Description based upon print version of record.

(2012), ‘Cyber security standards, practices and industrial •
applications’, in Athar Mahboob & Junaid Ahmed Zubairi, ed., IGI Global
(701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA), Hershey,
Pa, Restricted to subscribers or individual electronic text purchasers.

(2016), ‘African Data Privacy Laws’(33), in Alex B. Makulilo, ed., •
Springer International Publishing, Cham.

Martellini, M. (2013), ‘Cyber Security’, Springer, Dordrecht, • Includes bibliographical references.

Oltramari, R.; Cranor, L. F.; Walls, R. J. & Mcdaniel, P. (), ‘Building • an Ontology of Cyber Security’.

Pandya, P. (2014), ‘Advanced Data Encryption’, 325-345. •

Pino, R. E. (2014), ‘Network Science and Cybersecurity’(55), • Springer, New York, NY, Description based upon print version of record.

Pirc, W. G. (2011), ‘Cybercrime and Espionage’, Elsevier • monographs, [s.l.], Includes index.

(2010), ‘Insider Threats in Cyber Security’(49), in Christian W. • Probst, ed., Springer Science + Business Media, LLC, Boston, MA, Includes bibliographical references.

Saleem, M. (2019), ‘Brexit Impact on Cyber Security of United • Kingdom’.

Sankardas Roy, D. D. (2011), ‘Game Theory for Cyber Security’. •

Schneier, B. (2013), ‘Economics of Information Security and • Privacy III’, Springer, New York, NY, Description based upon print version of record.

Sevis, K. N. & Seker, E. (2016), ‘Cyber warfare: terms, issues, laws • and controversies’.

Shakarian, P.; Shakarian, J. & Ruef, A. (2013), ‘Introduction to • cyber-warfare’, Elsevier Science, Burlington, Description based upon print

version of record.

Shimonski

, R. (2014), ‘Cyber Reconnaissance, Surveillance and Defense’,•
Elsevier Science, Burlington, Description based upon print version of record.

Singhal, A. (2007), ‘Data Warehousing and Data Mining •
Techniques for Cyber Security’(31), Springer, [Berlin, Includes
bibliographical references and index.

(2015), ‘Smart grid security’, in Florian Skopik & Paul Smith, ed., •
Elsevier Science, Burlington, Description based upon print version of record.

(2018), ‘Cyber Situational Awareness in Public-Private- •
, Springer‹Partnerships’, in Florian Skopik; Tímea Páhi & Maria Leitner, ed.
Berlin Heidelberg, Berlin, Heidelberg.

Sood, A. (2014), ‘Targeted Cyber Attacks’, in Richard Enbody, ed., •
Elsevier Science, Burlington, Description based upon print version of record.

(2008), ‘Information security’, in Detmar W. Straub; Seymour E. •
, M.E. Sharpe, Armonk, N.Y, Includes‹Goodman & Richard Baskerville, ed.
bibliographical references and index.

Stuart, S. (2013), ‘My Revision Notes OCR Cambridge Nationals in •
, Hodder Education, London,‹ICT Levels 1’, in Brian Gillinder, ed.
Description based upon print version of record.

Tam, K. & Jones, K. (2018), ‘Cyber-Risk Assessment for•
Autonomous Ships’.

Taplin, R. (2016), ‘Managing Cyber Risk in the Financial Sector’, • Taylor and Francis, s.l., Description based upon print version of record.

(2003), ‘Information security management handbook’, in Harold F. • , Auerbach, Boca Raton, Fl, Includes‘Tipton & Micki Krause, ed. bibliographical references and index.

Vacca, J. R. (2014), ‘Cyber Security and IT Infrastructure • Protection’, Elsevier Science, Burlington, Description based upon print version of record.

Ventre, D. (2013), ‘Cyber Conflict’, Wiley, London, Description • based upon print version of record.

Wang, J. & Kissel, Z. A. (2015), ‘Introduction to network security’, • Wiley, Hoboken, Description based upon print version of record.

Wood, D.; Kohun, F.; Ali, A.; Paullet, K. & Davis, G. (2010), • ‘Cyber Forensics and Security ‘.

Yang, C. (2013), ‘Intelligent systems for security informatics’, • Academic Press, Oxford, Includes bibliographical references and index.

Ye, N. (2008), ‘Secure computer and network systems’, J. Wiley & • Sons, Chichester, England, Includes bibliographical references and index.

Onwubiko, C., ed., (2016), Cyber Science 2016, Centre for • Multidisciplinary Research, Innovation and Collaboration, [Woodford, London].

Gareth Jenkins, Technology or workforce: what's the greatest • security threat to business services? (November 2019) https://www.globalservices.bt.com

Margaret Rouse, (data breach), • https://searchsecurity.techtarget.com/definition/data-breach

Deep web cults, (https://accidentalfactory.com/deep-web- • investigation-and-secrets/cults/)

Antony Funnell, 1984 and our modern surveillance society, Jul • 2014, Future Tense

Chemi Shalev, (May 2018) Analysis Trump, Facebook, Cambridge • Analytica and the Appearance of 1984, (https://www.haaretz.com/israel-news/.premium-trump-facebook-cambridge-analytica-and-the-rise-of-1984)

Ernest Moniz and Sam Nunn, Cyber attacks and rising risks of an • accidental nuclear war, (https://www.straitstimes.com/opinion/cyber-attacks-and-rising-risks-of-an-accidental-nuclear-war), Feb, 2018

Nick Ismail, Poor cyber defence could lead to 'nuclear war',• (https://www.information-age.com/poor-cyber-defence-lead-nuclear-war-123466195/)

Nicole Lindsey, (October, 2019) Smart Devices Leaking Data To • Tech Giants Raises New IoT Privacy Issues (https://www.cpomagazine.com/data-privacy/)

Michael Baxter (October, 2019), IoT and privacy, IoT and data • insights: four considerations, (https://www.information-age.com/iot-privacy-

data-insights-four-123485898/)

Nick Ismail, (February 2020) Election hacking: is it the end of •
democracy as we know it? (https://www.information-age.com/election-hacking-end-democracy-123487698/)

Fredric Paul, Network World, Jun, 2019»IoT security vs. privacy: •
Which is a bigger issue?»,
(https://www.networkworld.com/article/3401522/iot-security-vs-privacy-which-is-a-bigger-issue.html)

Sumit Paul-Choudhury, (March 2019), •
(http://www.bbc.com/culture/story/20190318-how-the-apocalypse-could-be-a-good-thing)

Ian Crouch, (2013) So Are We Living in 1984? •
(https://www.newyorker.com/books/page-turner/so-are-we-living-in-1984)

W. Broad, J. Markoff, and D. Sanger, «Israeli Test on Worm Called•
D. Kushner,» New York Times, 15 Jan 11. • ‘Crucial in Iran Nuclear Delay
B.» IEEE Spectrum 53, No. 3, 48 (2013). • ‘«The Real Story of Stuxnet
» Strategic‹Kesler, «The Vulnerability of Nuclear Facilities to Cyber Attack
K. Zetter, Countdown to Zero Day: Stuxnet and theInsights 10, 15 (2011). •
Launch of the World’s First Digital Weapon (Crown, 2014).

J. Grayson, «Stuxnet and Iran’s Nuclear Program» Physics 241, 7•
Mar 11

نبذة عن الكاتبين:

ندى الربيعي:

ولدت عام 1979 في بغداد - العراق، حاصلة على بكالوريوس بحوث علمية عام 2003 من الجامعة الملكية الهولندية في لايدن - هولندا وماجستير عام 2008 في الصيدلة من الجامعة الملكية الهولندية في أوترخت - هولندا. أكملت دراسات عليا تخصصية في إدارة الأعمال في هولندا، وحاصلة على ترخيص الحزام الأسود الدولي في إدارة الأعمال والمشاريع 2019. حائزة على جائزة ولقب سيدة أعمال هولندا (من أصول أجنبية) لعام 2015. وفي العام الذي تلاه تم اختيارها من ضمن مئة شخصية مؤثرة في هولندا لعام 2016. لها عدة مقالات في الصحف العربية والهولندية في الشأن العام والسياسة. تقدم حاليا رسالة دكتوراة في جامعة ماري لاند الأمريكية في إدارة الصحة العامة وتعمل في إدارة صيدليات في مناطق مختلفة في هولندا.

عباس الزبيدي:

ولد ببغداد عام 1979م، حصل على البكالوريوس عام 2001م من قسم الهندسة الطبية (جامعة النهرين) وحصل على الماجستير من نفس الجامعة سنة 2004م. عمل كأخصائي للرنين المغناطيسي والطب النووي وعمل تدريسيا في كلية هندسة الخوارزمي (جامعة بغداد). حصل على منحة (DAAD) لدراسة الدكتوراة في اختصاص هندسة المعلوماتية الطبية كتخصص عام وبهندسة تكنولوجيا القياسات الطبية اللاتلامسية لطب الأطفال من جامعة آخن التقنية - ألمانيا الاتحادية.

ساهم في إدخال تقنية التصوير الحراري الطبي للكشف المبكر عن سرطان الثدي في العراق، وبجهوده الذاتية ولأول مرة في البلاد. نشر أكثر من 50 بحثًا علميًا وكتابًا حول تكنولوجيا المعلوماتية الطبية والهندسة الطبية الحيوية. يهتم بمجالات الهندسة الحيوية والطبية وتقنيات الأطراف الصناعية ومعالجة الصور والإشارات الفيزيولوجية والطبية المختلفة.

وعمل كمصمم لأنظمة التصوير الطبي لحساب وكالة الفضاء الكندية (CSA) وباحث في جامعة ساسكاتشيوان الكندية.